602LAN SUITE 2004

Mail-Server/Viren-/Spamschutz/Firewall/Fax

Benutzerhandbuch

Exklusiv-Vertrieb für Deutschland, Österreich & Schweiz:

HAAGE & PARTNER Computer GmbH
Schlossborner Weg 7
61479 Glashütten
Deutschland

Telefon: (06174) 966 100
Telefax: (06174) 966 101

Internet: www.haage-partner.de oder www.software602.de

Händleranfragen: dealers@haage-partner.de

Inhaltsverzeichnis

Einführung in 602LAN SUITE 6
SMTP-Server 7
POP3-Server 7
Webmail-Client 7
Faxserver 7
Firewall 7
NAT 7
SOCKS 7
Proxy 7
IP-Filter 8
SSL (Secure Socket Layer) 8
WWW-Server 8
DHCP-Server 8
LDAP-Adressbuch 8
Virenschutz (Option) 8
Spamschutz 8
Filter für Anhänge 8
Update Manager 8
ActiveReports (Option) 9
Content Filter – Inhaltsfilter (Option) 9
Installation 10
Systemvoraussetzungen 10
Zusätzliche Hinweise und Anforderungen 10
Download 10
Installieren 10

Grundlegende Einrichtung 11
Internet-Verbindung einrichten 11
Permanente Verbindung 11
Einwahlverbindung 11
Einwahl-Details 11
Sekundäre Verbindung (VPN) 12
Einen Einwahl-Zeitplan einrichten 12
Benutzerkonten einrichten 14
Standarddomäne 14
Einen Benutzer erstellen 14
Benutzerrechte 15
Aliase 16
Einen Benutzer löschen 16
Benutzer importieren 16
Benutzer exportieren 16
Mail-Server konfigurieren 17
Grundkonfiguration 17
SMTP- und SSL-SMTP-Server-Einstellungen 17
Mails mit dem SMTP-Protokoll empfangen 17
Die Verarbeitungsmethode für Mails wählen 18
POP3-Server-Einstellungen 20
POP3- oder SSL-POP3-Server einschalten 20
Liste der POP3-Postfächer 20
Mails weiterleiten 21
Kopie der Mails auf dem POP3-Server hinterlassen 21
Virenschutz konfigurieren 22
Mailclient konfigurieren 24
Microsoft® Outlook Express 6.x einrichten 24
Microsoft® Outlook 2002 einrichten 24
Auf den Webmail-Client zugreifen 25

Webserver konfigurieren ... 26
WWW-Konfiguration ... 26
Benutzer-Ordner verwenden ... 26
Zugriffsfilter ... 27
Verzeichnis durchsuchen ... 27
Webserver-Inhalt aktualisieren ... 27
Einen SSL-Webserver einrichten ... 28
FastCGI-Anwendungen ... 29
Weitergeleitete Anwendungen (Mapped Applications) ... 29
Aliase ... 30
Faxserver konfigurieren ... 31
Allgemein ... 31
TAPI ... 32
602LAN SUITE-spezifische Modembefehle ... 32
Installation des SendFax-Clients ... 33
Fax mit SendFax-Client versenden ... 33
Fax mittels Mail versenden ... 33
Faxnummer-Format beim Versand mittels Mail ... 33
Fax als Mail mit Anhang versenden ... 34
Gemeinsamen Internet-Zugang konfigurieren (NAT) ... 35
Was ist Network Address Translation (NAT)? ... 35
NAT aktivieren ... 35
NAT-Konfiguration ... 36
LAN-Workstation-Einstellungen für NAT ... 36
Gemeinsamen Internet-Zugang konfigurieren (Proxy) ... 37
Die Proxies einrichten ... 37
Microsoft® Internet Explorer einrichten ... 38

Grundlegende Administration ... 39
Administration konfigurieren ... 39
Administration durch die Anwendung ... 39
Webbasierte Administration ... 40
Server-Aktivität protokollieren ... 42
Als Windows-Dienst installieren ... 44
Win-Dienst ... 44
Win98-Dienst ... 44
DHCP-Server einrichten ... 45
IP-Bereiche einrichten ... 45
DHCP-Optionen ... 45

Erweiterte Features ... 46
SMTP-Authentifikation & -Einstellungen ... 46
Erweiterte Sendeparameter ... 46
SMTP-Relay-Optionen ... 47
Webmail ... 48
Anmeldung beim Webmail-Client ... 48
Fenster des Webmail-Clients ... 48
Postfach ... 49
Eine neue Mail erstellen ... 50
Rechtschreibprüfung ... 50
Adressbücher ... 50
Optionen ... 52
Optionenmenü ... 52
Filterregeln ... 53
Spamschutz-Einstellungen ... 54
WAP-Zugriff ... 56
Voraussetzungen ... 56
Einrichtung ... 56

Spamschutz ... 57
Schutz mit DNS-Negativlisten (DNS-BL) ... 57
Schutz mit der SMTP Positiv-/Negativliste ... 58
Schutz mit dem Bayesian-Filter ... 58
Schutz durch persönliche Positiv- und Negativliste ... 60
Filter für Anhänge ... 61
Einrichtung des LDAP-Adressbuchs ... 61
LDAP ... 61
Microsoft® Outlook Express als LDAP-Client einrichten ... 62
Praktischer Nutzen von LDAP ... 62
602LAN SUITE Update Manager ... 62
ActiveReports ... 64
Arbeitsweise ... 64

Inhaltsfilter (Content Filter) ... 65
Filtermethoden ... 65
Statische URL Filterung: URL-Datenbanken ... 65
Dynamische Filterung - Artificial Content Recognition (ACR) ... 65
Konfiguration ... 66
Aktivierung ... 66
SafeSurf-Einstufungsinformation verwenden ... 66
ICRA PICS-Einstufungsinformation verwenden ... 66
Bereits eingestufte URLs cachen ... 66
URL-Cachegröße ... 67
URL-Cache-Verzeichnis ... 67
Gecachete URLs löschen, älter als ... 67
Regeln für Inhaltsfilter, Positiv- und Negativlisten ... 67
Erstellen einer Regel ... 68
Inhaltsfilter-Sensitivität ... 69
Arbeitsweise des 602LAN SUITE Content Filter ... 69

Erweiterte Zugriffskontrolle ... 70
NAT ... 70
Prinzip ... 70
Firewall ... 71
Aufbau von IP-Verbindungen und Zugriffsbeschränkung ... 71
Firewall-Einstellungen ... 72
SMTP/POP3/WWW/LDAP-Server mit der hohen oder mittleren Sicherheitsstufe verwenden ... 73
Angepasste Sicherheitsstufe ... 73
Proxy-Cache ... 75
Den lokalen Proxy-Cache verwenden - Register "Proxy-Server" ... 75
Cache vorladen ... 75
Übergeordneter Proxy-/Cache-Server ... 75
Site-Zugriffskontrolle ... 76
Beispiele: ... 76
Weitergeleitete Links ... 77
Funktionsweise ... 77
Vorteile: ... 77
Nachteile: ... 77
Einstellungen ... 77
Proxy-IP-Filter-Konfiguration ... 79
IP-Filter-Einstellungen – Beispiel 1 ... 80
IP-Filter-Einstellungen – Beispiel 2 ... 80
SSL-Konfiguration ... 82
Allgemein ... 82
Erweitert ... 83

Anhang 85
Befehlssatz Hayes-kompatibler Modems 85
Beispiel für Mail-Einstellungen 87
Problemlösungen 88

Einführung in 602LAN SUITE

602LAN SUITE besteht grundsätzlich aus mehreren Server-Anwendungen, die optimal aufeinander abgestimmt sind. Die einzelnen Server können jederzeit ein- oder ausgeschaltet werden. Oft beginnt man mit dem Mail-Server und schaltet Dienste wie Fax-Server, gemeinsame Internetnutzung, Firewall, Spamfilter, DHCP-Server u.a. erst später dazu.

602LAN SUITE ist für bis zu 3 Benutzer kostenlos. Lizenzen für weitere Benutzer, den zusätzlichen Virenschutz und das Statistikmodul können Sie in unserem Shop erwerben: shop.haage-partner.de

602LAN SUITE wird ausschließlich für die Windows-Plattform entwickelt. Einige Funktionen, wie Firewall und NAT, sind unter Windows 98/ME nicht verfügbar.

Sie können die neueste Version von 602LAN SUITE auf der Webseite www.software602.de laden.

Die Hauptfunktionen der 602LAN SUITE

- **Sicherer Mail-Server**
  - Virenschutz (optional)
  - Filter für Anhänge schützt vor gefährliche Viren
  - Spamschutz (Bayesian-Filter, Postitiv/Negativlisten, Blocklisten)
  - gemeinsames Adressbuch über LDAP
  - Webmail-Client für den weltweiten Zugriff
  - SMTP- und SSL-SMTP-Server
  - POP3- und SSL-POP3-Server

- **Fax-Server** für alle Arbeitsplätze
  - unterstützt Faxmodem (TAPI) und ISDN (CAPI)

- **Gemeinsame Internetnutzung** für alle Arbeitsplätze
  - einfache Einrichtung mit NAT (Network Address Translation)
  - Proxy mit Cache für HTTP/HTTPS/HTTP-FTP, FTP, SOCKS, Telnet und RealAudio
  - **Content Filter** - Inhaltsfilter (optional, neu in Version 2004)

- **Netzwerksicherheit**
  - Firewall
  - IP-Filter
  - Filter für Dateianhänge

- **Webserver**
  - SSL, ISAPI-, CGI- und FastCGI-Zugriff

- **DHCP-Server**
- **Update Manager** (neu in Version 2004)
- **ActiveReports** (optional, neu in Version 2004)

Beschreibung der Funktionen

SMTP-Server

Eine der Hauptfunktionen der 602LAN SUITE ist das direkte Versenden und Empfangen von Mails mit dem SMTP-Protokoll. 602LAN SUITE kann direkt als Mail-Server für das Internet arbeiten, ohne einen entsprechenden Dienst des Internetanbieters zu benötigen. Mit dieser Methode liefert der Server Mails aus dem Internet direkt an die Benutzerpostfächer. Zusätzlich überwacht er den Port, der für das SMTP-Protokoll belegt ist (standardmäßig Port 25). Wenn eine Mail ankommt, handhabt der Server alles Weitere. Sie können zusätzlich für den SMTP-Server SSL einrichten, um eine sichere Kommunikation zwischen Server und Client zu gewährleisten.

POP3-Server

602LAN SUITE arbeitet als POP3-Server mit optionaler SSL-Verschlüsselung , um Zugriff auf die Mails in den Benutzerpostfächern von einem Mail-Programm zu ermöglichehn. Es können beliebige Mail-Programme unter Windows, MacOS oder Linux verwendet werden, beispielsweise Microsoft Exchange, Outlook Express, Netscape Messenger, Eudora, KMail oder Evolution. Für die sichere Kommunikation zwischen Server und Client können Sie für den POP3-Server eine SSL-Verschlüsselung einrichten.

Webmail-Client

Der Webmail-Client macht die Benutzerpostfächer über einen beliebigen Webbrowser zugänglich. Die gesamte Kommunikation zwischen dem Browser und dem 602LAN SUITE-Server wird dabei über das HTTP- oder verschlüsselt über das HTTPS-Protokoll gehandhabt.

Faxserver

Der Faxserver funktioniert mit Hilfe eines TAPI- (Faxmodem) bzw. CAPI-Geräts (ISDN). Eingehende Faxe werden anhand der Fax-IDs, die unter "Benutzer/Eigenschaften" angegeben werden, an die entsprechenden Benutzerpostfächer weitergeleitet. Faxe, die nicht zugeordnet werden können, werden an jeden Benutzer weitergeleitet, für den "Nicht zugeordnete Faxe an Benutzer weiterleiten" angewählt ist.

Firewall

Die Firewall schützt den Computer, auf dem 602LAN SUITE läuft, und das gesamte lokale Netzwerk (LAN) gegen unautorisierte TCP/IP-Verbindungen. Die Firewall von 602LAN SUITE basiert auf Regeln, die in Sets zusammengefasst werden. Wenn keine Regeln definiert sind, werden alle TCP/IP-Verbindungen abgewiesen.

NAT

NAT steht für Network Address Translation. Die Idee hinter NAT ist, den IP-Header umzuschreiben und die numerische Adresse durch eine andere zu ersetzen. NAT erlaubt einem einzelnen Dienst, wie z.B. den PC auf dem 602LAN SUITE installiert ist, als Verbindung zwischen dem Internet und dem lokalen (oder privaten) Netzwerk zu agieren. Das bedeutet, dass nur eine einzige IP-Adresse benötigt wird um eine ganze Reihe von PCs zu bedienen.

SOCKS

SOCKS wurde ursprünglich von David Koblas entwickelt und später zu seiner jetzigen Form (Version 5) verändert und erweitert. Es ist ein Protokoll, das TCP-Anfragen auf dem Computer über die Firewall leitet, damit Benutzer-Anwendungen auf transparente Weise die Firewall passieren können. Dieses Protokoll ist unabhängig von den Anwendungsprotokollen und kann daher für viele Dienste, wie Telnet, FTP, Gopher, WWW usw. verwendet werden. Der Server überträgt Daten zwischen Client und Server mit einer minimalen CPU-Belastung. Da SOCKS nicht auf Anwendungsprotokoll-Ebene arbeitet, kann es leicht mit Protokollen verwendet werden, die ihre Datenübertragung verschlüsseln.

Proxy

Ein Proxy hat den Vorteil, dass nur eine IP-Adresse benötigt wird, um das gesamte lokale Netzwerk mit dem Internet zu verbinden ohne dass ein Hardware-Router benötigt wird. Der Proxy von 602LAN SUITE bietet Caches für die verschiedenen unterstützten Protokolle. Das Client-Programm muss die Kommunikation über einen Proxy unterstützen. Der Proxy von 602LAN SUITE unterstützt HTTP/HTTPS/HTTP-FTP, FTP, SOCKS, Telnet, RealAudio und HTTP-Caching. 602LAN SUITE unterstützt einen sekundären Proxy- oder Cache-Server (nur HTTP/HTTPS/HTTP-FTP), der seine Daten über einen weiteren Proxy/Cache-Server erhält, der zum Beispiel beim Internetanbieter untergebracht sein kann.

IP-Filter

Der IP-Filter prüft TCP/IP-Pakete anhand ihrer IP-Adresse und entscheidet, ob ihnen Zugang zu einem bestimmten Dienst gestattet werden soll.

SSL (Secure Socket Layer)

Das TCP/IP-Protokoll transportiert und leitet Daten über das Internet. Andere Protokolle wie das HyperText Transport Protocol (HTTP), das Lightweight Directory Access Protocol (LDAP) oder das Simple Mail Transfer Protocol (SMTP) nutzen das Basisprotokoll TCP/IP, um typische Anwendungsaufgaben, wie das Empfangen von Webseiten, zu realisieren. SSL läuft oberhalb von TCP/IP und unterhalb des Anwendungsprotokolls wie HTTP oder SMTP, um mit verschiedenen Anwendungsprotokollen verschlüsselte Verbindungen zu ermöglichen. So gestattet es einem SSL-basierten Server sich bei einem Client (z.B. Webbrowser), der SSL unterstützt, zu authentifizieren.

WWW-Server

Der WWW- (World Wide Web) und der SSL-WWW-Server liefern HTML-Seiten, die in einem bestimmten Verzeichnis (siehe "WWW/Startverzeichnis des WWW-Servers") gespeichert sind, an Webbrowser.

DHCP-Server

Das DHCP-Protokoll (Dynamic Host Configuration Protocol) gibt 602LAN SUITE die Möglichkeit, einem Client-PC dynamisch eine IP-Adresse und andere TCP/IP-Parameter zuzuweisen. Die DHCP-Parameter können vom Administrator in der erweiterten Konfiguration unter "DHCP" eingestellt werden.

LDAP-Adressbuch

Das LDAP-Protokoll ist ein Standard-Client-Server-Protokoll um Informationen in LDAP-Servern anzuzeigen. Der LDAP-Verzeichnisdienst ist ein mächtiges Werkzeug für die weltweite Suche von Personen und Firmen. 602LAN SUITE enthält einen LDAP-Server um Benutzerinformationen anzubieten. Wenn dem LDAP-Adressbuch eine bestimmte Adresse hinzugefügt werden soll, aktivieren Sie für den entsprechenden Benutzer unter "Benutzer/Eigenschaften" die Option "Hinzufügen in Liste für LDAP-Adressbuch". Jeder Mail-Client, der einen LDAP-Client enthält (wie Outlook Express) kann auf alle Mail-Adressen, die im LDAP-Adressbuch enthalten sind, zugreifen.

Virenschutz (Option)

602LAN SUITE Antivirus-Edition kann ankommende und ausgehende Mails mit Hilfe der **BitDefender**-Technologie auf Viren prüfen. Alle eingehenden Mails werden mitsamt eventuellen Anhängen auf Viren und Würmer geprüft, bevor Sie in die Benutzer-Postfächer gelangen.

Die BitDefender-Engine wurde von den ICSA Labs und den West Coast Labs zertifiziert, erhielt mehrere VB 100%-Auszeichnungen und bietet eine außergewöhnlich hohe Scangeschwindigkeit und Erkennungsrate.

Spamschutz

Der Spamschutz hindert unerwünschte Mails daran, in Ihr Netzwerk einzudringen. 602LAN SUITE bietet vier Spamschutz-Methoden an. Erstens einen Bayesian-Filter, zweitens DNS-Negativlisten (DNS-BL), drittens auf dem Server basierende Positiv/Negativ-Listen und viertens benutzerdefinierte Positiv/Negativ-Listen.

Filter für Anhänge

Der Filter für Anhänge kann Mails auf anhängende Dateien mit speziellen Dateiendungen überprüfen. Eine Mail mit einem ungewollten Anhang kann geliefert, ohne den Anhang geliefert, nicht geliefert oder in einem speziellen Postfach abgelegt werden. Gefährliche Dateien, wie z.B. EXE, PIF, BAT können so direkt gelöscht werden, bevor sie Schaden anrichten.

Update Manager

602LAN SUITE unterstützt die automatische Update-Prüfung. Wenn ein neues Update verfügbar ist, kann 602LAN SUITE dieses herunterladen und den Administrator informieren.

ActiveReports (Option)

ActiveReports bietet eine umfassende Analyse der 602LAN SUITE-Nutzung. Es vereinfacht die Kontrolle der Benutzung, des Datenverkehrs, der Einlogzeiten, der besuchten Seiten, der Virenaktivitäten und vieles mehr. ActiveReports kann zusätzlich erworben werden. ActiveReports ist eine Erweiterung der 602LAN SUITE und kann 30 Tage kostenlos getestet werden.

Content Filter – Inhaltsfilter (Option)

Der 602LAN SUITE Content Filter ist ein optionales Zusatzmodul, das die Filterung unerwünschter Webinhalte ermöglicht. Der Filter kann 30 Tage kostenlos getestet werden.

Installation

Systemvoraussetzungen

Betriebssystem
Windows 98SE/ME/NT/2000/XP/2003 (ein MS Windows-Server-Betriebssystem ist nicht erforderlich!)

Speicher
Windows 98SE/ME – 32 MB RAM
Windows NT/2000/XP – 64 MB RAM
Windows 2003 – 128 MB RAM

Festplattenspeicher
30 MB für 602LAN SUITE + etwa 10MB pro Benutzerpostfach

Zusätzliche Hinweise und Anforderungen

- Um 602LAN SUITE zu verwenden, benötigen Sie ein einwandfrei arbeitendes TCP/IP-Netzwerk. Alle Clients und Server müssen in der Lage sein, über das TCP/IP-Protokoll fehlerfrei miteinander zu kommunizieren, bevor Sie 602LAN SUITE installieren. Der Server, auf dem Sie 602LAN SUITE installieren, muss mit dem Internet verbunden sein und auf Internet-Dienste zugreifen können.
- Microsoft Internet Explorer 5.0 oder neuer wird benötigt, um alle Funktionen zu nutzen. Mindestens die Version 4 wird benötigt, um mittels Proxy auf das Internet zuzugreifen.
- Die Betriebssystem Windows 98 und Windows ME unterstützen mit 602LAN SUITE als Netzwerk-Server nicht mehr als 10 Benutzer zuverlässig. Diese Betriebssysteme sind Desktop-Betriebssysteme und nicht für Server-Anwendungen gedacht oder entworfen. Für Netzwerke mit mehr als 10 Computern empfehlen wir den Einsatz von Windows NT/2000/XP/2003 für den 602LAN SUITE-Server.
- Die Firewall- und NAT-Funktionalität ist nur unter Windows 2000/XP/2003 verfügbar. Computer mit multiplen Prozessoren oder Prozessoren die Hyper-Threading unterstützen, steht die Firewall- und NAT-Funktionen nicht zur Verfügung.
- Die Antivirus-Edition beinhaltet ein Jahr Virenschutz-Updates (ab dem Zeitpunkt der Aktivierung).

Download

Sie können die aktuelle Version der 602LAN SUITE von www.software602.de laden.

Installieren

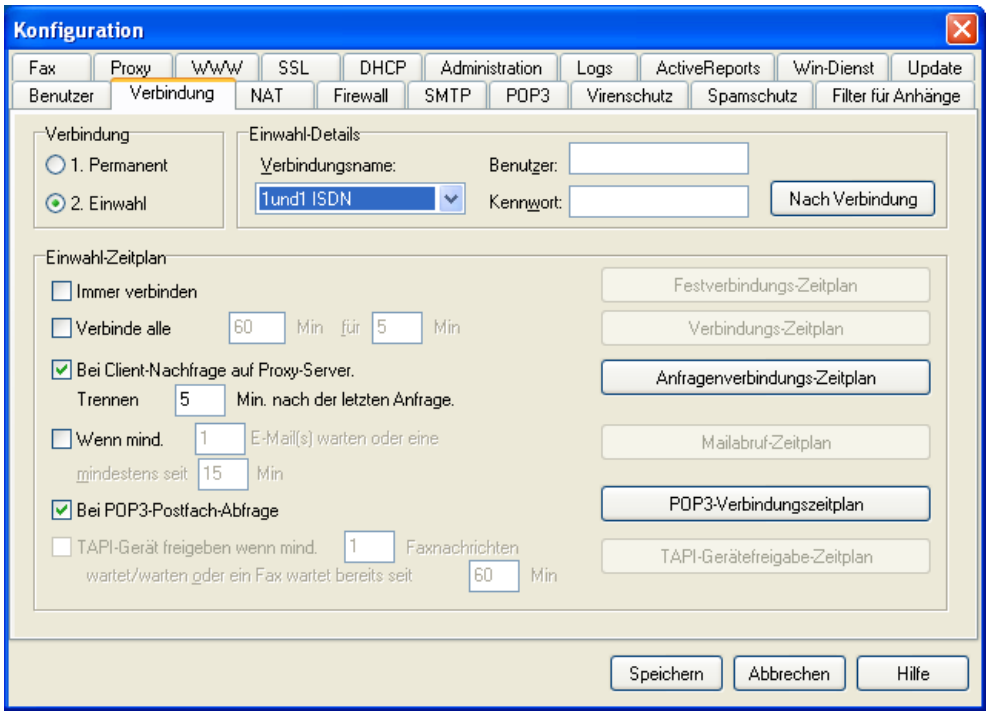
1. Starten Sie ls2004.exe.
2. Folgen Sie den Anweisungen des Installationsprogramms.
3. Nachdem Sie den Lizenzbestimmungen zugestimmt haben, wählen Sie den Ordner für die Programminstallation oder bestätigen Sie die Vorgabe (C:\Programme\Software602\602LAN SUITE).
4. Wählen Sie danach den Namen des Ordners für die Symbole im Startmenü oder bestätigen Sie die Vorgabe.
5. Nun werden alle Dateien in den gewählten Ordner kopiert.
6. Die Installation von 602LAN SUITE ist danach abgeschlossen.

Weitere Hilfe finden Sie auf unserer Supportseite oder in unserer Registrierungs- und Aktualisierungsanleitung.
Unsere Supportseite finden Sie unter: www.software602.de

Grundlegende Einrichtung

Internet-Verbindung einrichten

Unter "Verbindung" können Sie angeben, wie Ihr Server mit dem Internet verbunden wird. Starten Sie 602LAN SUITE, wählen Sie "Einstellungen" und dann "Erweiterte Konfiguration" aus dem Menü und aktivieren Sie "Verbindung". Es gibt dort zwei grundlegende Optionen, die von der verwendeten Verbindungsart abhängig sind.



Permanente Verbindung

Wenn die Verbindung über eine permanente Leitung erfolgt (DSL, Kabelmodem, Standleitung), ist es nicht nötig, vor jedem Internet-Zugriff erneut eine Verbindung aufzubauen. Wählen Sie in diesem Fall die Position 1 "Permanent". Wählen Sie diese Methode auch, wenn Sie nicht über eine permanente Leitung verbunden sind, die Internet-Verbindung aber durch einen anderen Computer hergestellt wird. Diese Auswahl bedeutet, dass sich das Programm nicht um die Internet-Verbindung kümmert, sondern davon ausgeht, dass diese bereits besteht. In diesem Fall sind alle weiteren Optionen in diesem Register schattiert und damit inaktiv.

Einwahlverbindung

Wenn Sie eine Einwahlverbindung (analoge Modem-Einwahl oder ISDN) nutzen, um eine Internet-Verbindung herzustellen, und Sie möchten, dass 602LAN SUITE die Internet-Verbindung automatisch aufbaut und beendet, dann wählen Sie Option 2 "Einwahl". Definieren Sie über den "Einwahl-Zeitplan", unter welchen Bedingungen eine Verbindung aufgebaut und wann sie wieder beendet wird und geben Sie bei "Einwahl-Details" die gewünschte Verbindung und die Anmelde-Informationen an. 602LAN SUITE funktioniert mit jeder Windows-Einwahlverbindung.

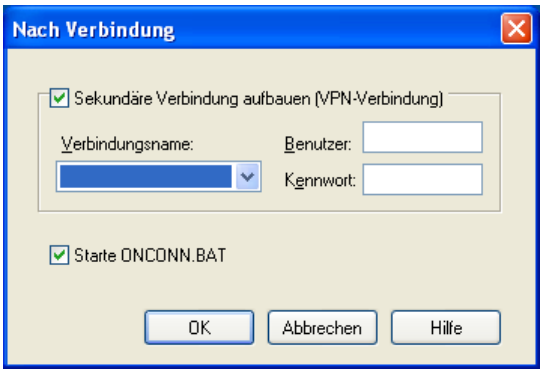
HINWEIS: Eine Einwahlverbindung MUSS zuerst unter Windows (Systemsteuerung/Netzwerkverbindungen) konfiguriert werden, bevor Sie sie mit 602LAN SUITE verwenden können!

Einwahl-Details

Wählen Sie in der Liste "Verbindungsname" den Namen des Profils für die Einwahlverbindung, die Sie verwenden möchten, um eine Internet-Verbindung aufzubauen. Tragen Sie den Benutzernamen und das Kennwort ein, mit dem Sie auf die Verbindung zugreifen. Sie erhalten diese Daten von Ihrem Internetanbieter.

Sekundäre Verbindung (VPN)

Um eine sekundäre Verbindung (VPN-Verbindung) zu konfigurieren klicken Sie die Schaltfläche "Nach Verbindung". Ein VPN (Virtuelles Privates Netzwerk) ist ein Weg, um durch Verschlüsselung und Authentifizierung eine private Verbindung aufzubauen oder durch ein öffentliches Netzwerk zu „tunneln“. Es ist notwendig, den VPN-Adapter in Windows 98 oder höher in "Systemsteuerung/Netzwerk" zu konfigurieren. Stellen Sie sicher, dass der VPN-Adapter vorhanden ist. Klicken Sie die Schaltfläche "Nach Verbindung", aktivieren Sie "Sekundäre Verbindung aufbauen", wählen Sie eine zuvor in Windows erstellte Verbindung und geben Sie die entsprechenden Anmelde-Informationen ein.



Die Batchdatei "ONCONN.BAT" wird verwendet, um die Routentabelle zu ändern oder einen anderen Batchprozess zu starten. Wenn Sie mit der VPN-Verbindung einen Prozess laufen lassen müssen, erstellen Sie die Datei "ONCONN.BAT", speichern Sie sie in den Ordner, in dem 602LAN SUITE installiert ist und aktivieren Sie die Option "Starte ONCONN.BAT".

HINWEIS: Zur Zeit unterstützt 602LAN SUITE eine VPN-Verbindung nur über ein zweites Modem. PPTP-Verbindungen über das Internet werden nicht unterstützt.

Einen Einwahl-Zeitplan einrichten

Festverbindung

Für eine permanente Einwahlverbindung ins Internet wählen Sie "Festverbindung". Dies aktiviert die Schaltfläche "Festverbindungs-Zeitplan". Klicken Sie auf diese Schaltfläche, um eine Tabelle zu öffnen, in der Sie angeben können, zu welchen Zeiten in der Woche die Verbindung aufgebaut werden soll. Die Tabelle ist in Intervalle zu je einer halben Stunde aufgeteilt. Bei einem grünen Feld wird eine Verbindung aufgebaut, bei einem roten Feld ist keine Verbindung erlaubt.

Periodische Verbindungen

Wählen Sie "Verbinde alle", um in regelmäßigen Abständen für eine bestimmte Zeit eine Internet-Verbindung aufzubauen. Geben Sie das Intervall in Minuten in das rechts danebenliegende Feld und die minimale Verbindungsdauer in das darauf folgende Feld ein. Klicken Sie die Schaltfläche "Verbindungs-Zeitplan", um eine Tabelle zu öffnen, in der Sie angeben können, zu welchen Zeiten in der Woche die Verbindung aufgebaut werden soll. Bei einem grünen Feld kann eine Verbindung aufgebaut werden, bei einem roten Feld ist keine Verbindung erlaubt.

Bei Client-Nachfrage auf Proxy-Server

Wählen Sie "Bei Client-Nachfrage auf Proxy-Server", um bei einer Client-Nachfrage für SOCKS-, DNS oder irgendeinen Proxy-Dienst eine Internet-Verbindung aufzubauen. Geben Sie die Anzahl der Minuten an, nach denen eine bestehende Verbindung nach der letzten Anfrage getrennt werden soll.

Wenn mindestens x Mails warten

Wählen Sie diese Option, wenn Sie möchten, dass 602LAN SUITE eine Internet-Verbindung aufbaut, wenn x Mails x Minuten lang warten. Verwenden Sie den "Mailabruf-Zeitplan" um festzulegen, wann 602LAN SUITE diese Regel befolgen soll.

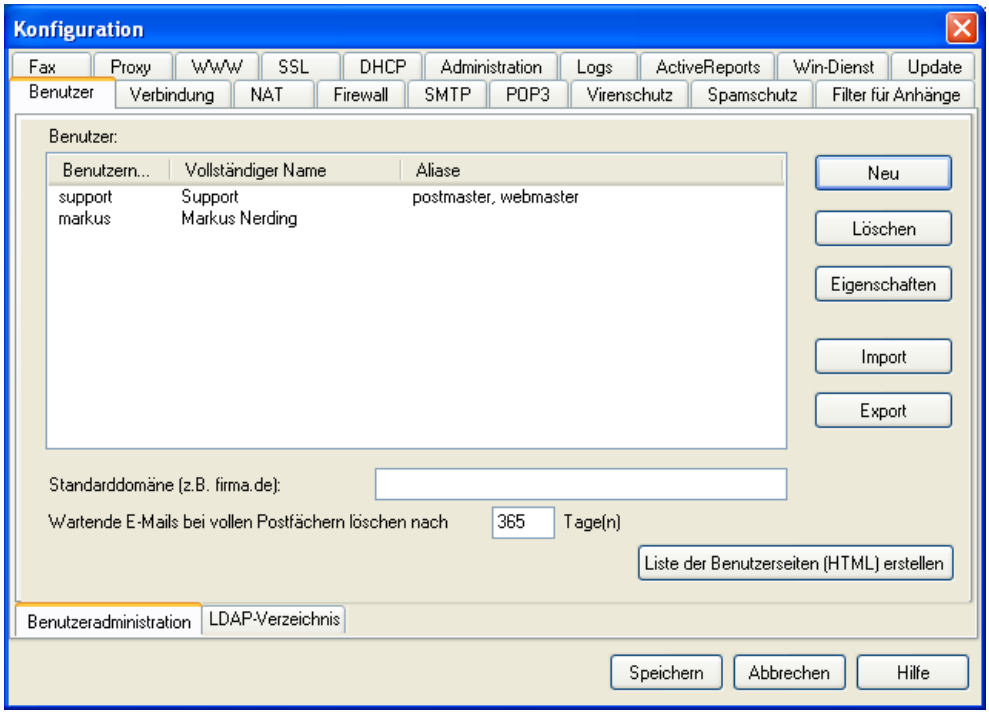
Bei POP3-Postfach-Abfrage

Verwenden Sie diese Option, damit 602LAN SUITE eine Internet-Verbindung aufbaut, wenn ein POP3-Postfach, das im Register "POP3" angegeben, abgefragt werden soll. Verwenden Sie den "POP3-Verbindungszeitplan" um festzulegen, wann 602LAN SUITE diese Regel befolgen soll.

TAPI-Gerät freigeben, wenn mindestens x Faxnachrichten warten
Diese Einstellung erlaubt es 602LAN SUITE, sowohl für den Internet-Zugriff als auch für das Faxen ein einzelnes Modem zu verwenden. Wenn eine bestimmte Anzahl von Faxen auf den Versand wartet, wird 602LAN SUITE automatisch die Internet-Verbindung so lange unterbrechen, bis die Faxe versendet wurden. Danach wird wieder die Internetverbindung aufgebaut.

Benutzerkonten einrichten

Sie finden das Register "Benutzer", indem Sie aus dem Menü von 602LAN SUITE "Einstellungen" und dann "Erweiterte Konfiguration" wählen. Benutzerkonten werden für die Mail- und Fax-Dienste, sowie die Proxy-Authentifierung benötigt. Ein falsches Einrichten von Benutzerkonten kann den Verlust von Mails verursachen oder sogar den Zugriff auf das 602LAN SUITE-Programm komplett sperren!



HINWEIS: Richten Sie immer zuerst das Administrator-Konto ein!

Standarddomäne

Wann Sie eine Standarddomäne verwenden sollten

Verwenden Sie eine Standarddomäne, wenn Sie 602LAN SUITE als Mail-Server für Ihre registrierte Domäne (z.B. ihre-firma.de) verwenden möchten. Eine Standarddomäne lässt 602LAN SUITE wissen, für welche Internet-Domäne das Programm Mail-Dienste anbietet.

Wann Sie keine Standarddomäne verwenden sollten

Wenn Sie 602LAN SUITE nur intern für Mails verwenden oder nur Mail-Adressen von Ihrem Internet-Anbieter verwenden, die mit dessen Domänennamen enden, benötigen Sie keine Standarddomäne. Verwenden Sie in diesem Fall Aliase (siehe Abschnitt "Einen Benutzer erstellen").

Wartende Nachrichten bei vollen Postfächern nach x Tagen löschen

Diese Option wird nur berücksichtigt, wenn ein Benutzerpostfach sein Größenlimit erreicht hat und über POP3-Sammeln weitere Mails für diese Mailbox eingehen oder weitere Faxe empfangen werden. Wenn mittels SMTP eine Mail an ein Benutzerpostfach gesendet wird, das sein Größenlimit erreicht hat, wird an den versendenden SMTP-Server der Standard-SMTP-Fehler 450 „Postfach voll“ bzw. „mailbox full“ zurückgegeben. Dieser wird dann in der Regel dem Absender eine Fehlermeldung zurückschicken.

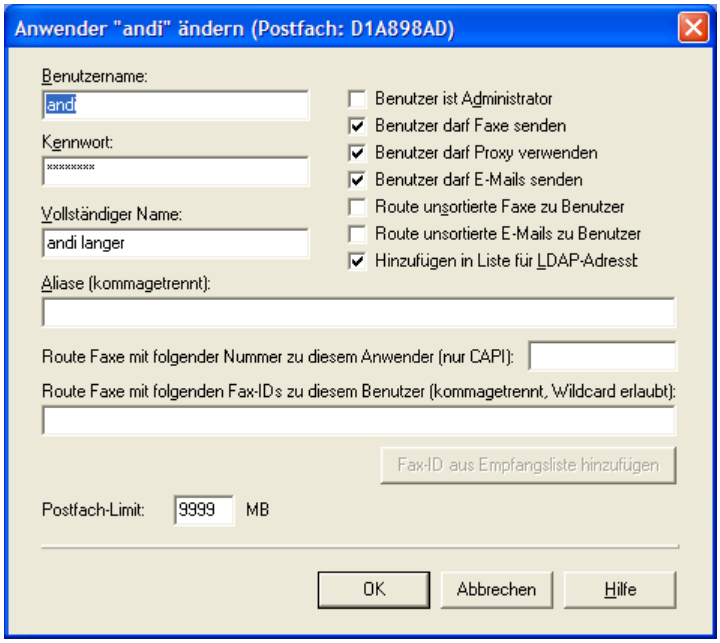
Einen Benutzer erstellen

Klicken Sie "Neu", um ein neues Benutzerkonto zu erstellen:

- **Benutzername** – Geben Sie den Benutzernamen an. Der Name wird als Namensteil der Mail-Adresse verwendet. Wenn Sie als Standarddomäne "firma.de" eingaben und der Benutzername "klaus" ist, wird dessen Mail-Adresse "klaus@firma.de" lauten. Benutzernamen dürfen nur gültige Zeichen enthalten. Verwenden Sie in einem Benutzernamen nicht das @-Symbol. Andernfalls ist der Benutzername ungültig und der Benutzer kann sich nicht anmelden, um Dienste von 602LAN SUITE zu verwenden. **HINWEIS:**

Standardmäßig können nur eingetragene 602LAN SUITE-Benutzer 602LAN SUITE zum versenden von Mails verwenden (siehe "SMTP/SMTP-Relay").

- **Kennwort** – Geben Sie ein Kennwort ein. Die Kennwortabfrage achtet nicht auf Groß- und Kleinschreibung. Das Kennwort wird nur versteckt angezeigt (je Zeichen ein Stern). Zeichen mit Akzent u.ä. sind nicht erlaubt.
- **Vollständiger Name** – Geben Sie den vollständigen Namen ein. Er wird zur besseren Identifikation in der Benutzerliste angezeigt.
- **Aliase** – Wenn die Mail-Adresse des Benutzers nicht dem Muster benutzername@standarddomäne entspricht oder der Benutzer von mehreren Mail-Adressen Mails empfängt, müssen Sie seine aktuelle Mail-Adressen oder seine zusätzliche(n) Mail-Adresse(n) angeben. Dabei sind nur komplette Mail-Adressen wie irgendjemand@firma.de sinnvolle Aliase, denn wenn nur der Namensteil verwendet wird, wird als Domaine die Standarddomaine verwendet. Benutzen Sie Komma- oder Leerzeichen, um mehrere Aliase voneinander zu trennen.
- **Faxe mit folgenden Fax-IDs an diesem Benutzer leiten** – Alle eingehenden Faxe mit der eingegebenen Fax-ID werden an das Postfach des Benutzers ausgeliefert. Die Schaltfläche "Fax-ID aus Empfangsliste hinzufügen" öffnet ein Fenster mit einer Liste der Fax-IDs empfangener Faxe. Hier können Sie Fax-IDs wählen, die an den Benutzer weitergeleitet werden sollen. Benutzen Sie Komma oder Leerzeichen, um mehrere Fax-IDs voneinander zu trennen. "*" und "?" sind erlaubt, um Muster anzugeben.
- **Postfach-Limit** – Hier können Sie das Größenlimit für das Postfach des Benutzers angeben.



Benutzerrechte

Wenn Sie einen Benutzer hinzufügen, befinden sich auf der rechten Seite des Fensters folgende Optionen. Wählen Sie diejenigen an, die Sie für den betreffenden Benutzer verwenden möchten. **Stellen Sie sicher, mindestens einen Benutzer den Administrator-Status zu verleihen!**

- **Benutzer ist Administrator** – Der Benutzer hat das Recht, 602LAN SUITE lokal oder mittels Webbrowser (Fernadministration) zu verwalten.
- **Benutzer darf Faxe senden** – Der Benutzer hat das Recht, Faxe zu versenden.
- **Benutzer darf Proxy verwenden** – Diese Regel funktioniert nur, wenn im Register "Proxy" die Option "Authentifizierung erforderlich" angewählt ist. Wenn diese Option angewählt ist, erscheint ein Anmeldefenster, wenn ein Benutzer auf den HTTP/HTTPS/HTTP-FTP-Proxy zugreifen möchte. Der Benutzer erhält das Recht, den Proxy zu verwenden, wenn er sich mit korrektem Benutzername und Kennwort anmeldet und die Option "Benutzer darf Proxy verwenden" angewählt ist. Dies betrifft nicht den Zugriff auf die Proxies für SOCKS, FTP, Telnet und RealAudio.

- **Benutzer darf Mails senden** – Der Benutzer hat das Recht, Internet-Mails zu senden. Jeder 602LAN SUITE-Benutzer hat das Recht, lokale Mails zu verwenden, aber nur Benutzer, für die Sie diese Regel aktivieren, dürfen Mails mit 602LAN SUITE über das Internet versenden.
- **Nicht zugeordnete Faxe an diesen Benutzer** – Faxe mit IDs, die nicht in einer Faxroute enthalten sind, werden an alle Benutzer mit diesem Recht weitergeleitet. **HINWEIS:** Wenn nicht mindestens ein Benutzer dieses Recht hat, erhalten alle Benutzer nicht zugeordnete Faxe.
- **Nicht zugeordnete Mails an diesen Benutzer** – Mit POP3 empfangene Mails, die keinem Benutzer zugeordnet werden können, werden an alle Benutzer mit diesem Recht weitergeleitet. **HINWEIS:** Wenn nicht mindestens ein Benutzer dieses Recht hat, erhalten alle Benutzer nicht zugeordnete Mails.
- **Hinzufügen in LDAP-Adressbuch** – Wenn Sie diese Regel aktivieren, wird der Benutzer in das LDAP-Adressbuch aufgenommen.

Aliase

Sie können immer dann einen Alias verwenden, wenn die Mail-Adresse des Benutzers nicht mit benutzername@standarddomäne übereinstimmt oder ein Benutzer Mails von mehr als einem Mail-Zugang empfängt.

Einen Benutzer löschen

Wählen Sie den Benutzer, den Sie entfernen möchten und klicken Sie "Löschen".

Benutzer importieren

Benutzer können mit Hilfe der Schaltfläche "Import" von einer CSV-Textdatei oder aus dem Pool der lokalen Windows NT/2000/XP-Benutzer importiert werden.

- **Benutzer von Textdatei (CSV) importieren** – Wählen Sie die CSV-Datei zum Importieren, wählen Sie die zu importierenden Felder und ordnen Sie jedem Feld das entsprechende 602LAN SUITE-Feld zu.
- **Windows NT/2000/XP-Benutzer importieren** – Wählen Sie die lokalen Windows-Benutzer, die Sie importieren möchten und klicken Sie auf "Ausgewählte Benutzer hinzufügen".

HINWEIS: Kennwörter für importierte Benutzer können einzeln für jeden Benutzer gesetzt werden oder Sie setzen ein Standard-Kennwort für alle Benutzer. Die Benutzer können ihre Kennwörter später mit dem Webmail-Client ändern.

Benutzer exportieren

Die Schaltfläche "Export" bietet die Möglichkeiten 602LAN SUITE-Benutzerinformationen (Benutzername, vollständiger Name, Mail-Adresse, Aliase, Benutzerrechte, Faxnummer, Fax-IDs und Postfach-Limit) zu speichern. Sie können die Liste in eine Textdatei mit Endung "TXT" oder Endung "CSV" (kommagetrennte Werte) exportieren.

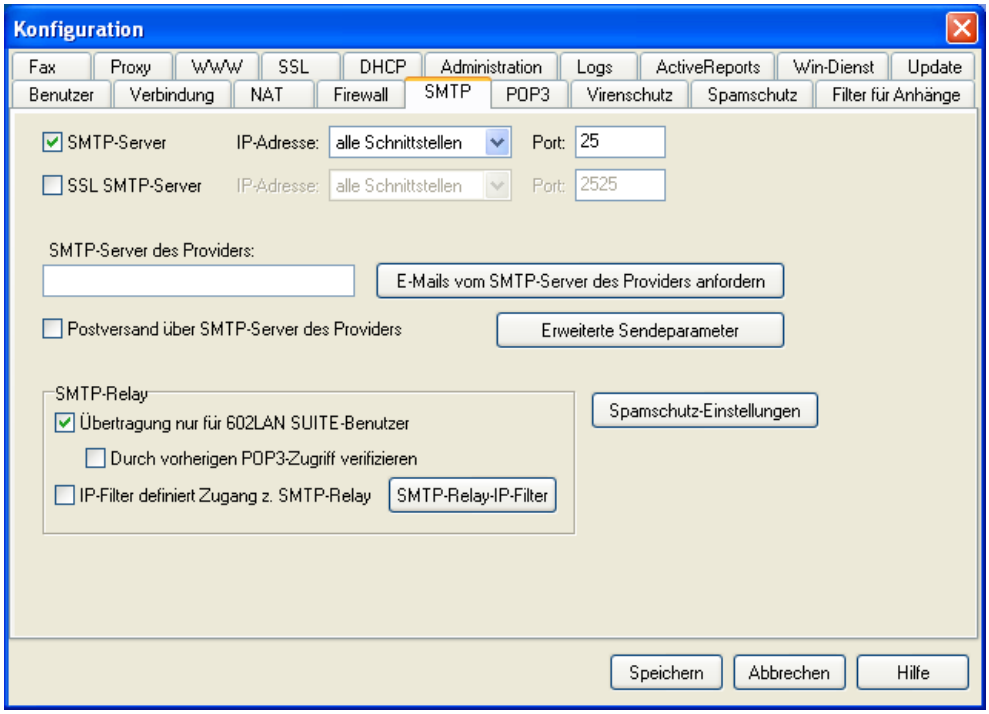
HINWEIS: Das Trennzeichen können Sie in den "Regionen- und Sprachoptionen" in der "Systemsteuerung" einstellen, indem Sie "Anpassen" klicken und das "Listentrennzeichen" bei "Zahlen" ändern.

Mail-Server konfigurieren

Grundkonfiguration

Das Register "SMTP" lässt Sie die Parameter einstellen für die Übertragung von Mails mit dem SMTP-Protokoll einstellen. Das Versenden von Mails mit SMTP ist klar geregelt - wenn eine Mail wartet und das Arbeitsintervall erreicht ist (siehe "Erweiterte Sendeparameter") wird die Mail versendet. Um Mails mit SMTP zu empfangen, ist es erforderlich, 602LAN SUITE entsprechend zu konfigurieren. Mitunter muss auch Ihr Internetanbieter/Domänenanbieter die ein oder andere Einstellung vornehmen.

HINWEIS: Bevor Sie den SMTP-Server konfigurieren, um Mails zu senden oder zu empfangen, legen Sie bitte die Benutzerkonten und deren Mail-Adressen, wie in "Benutzerkonten einrichten" beschrieben, an.



SMTP- und SSL-SMTP-Server-Einstellungen

Es ist möglich, den kompletten SMTP-Server über das Auswahlfeld "SMTP-Server" ein- oder auszuschalten. Sie können auch die IP-Schnittstellen anwählen, auf denen der SMTP-Server arbeiten soll. Standardmäßig sind alle lokalen Schnittstellen aktiviert, doch Sie können auch eine bestimmte IP-Adresse auswählen. So können Sie den SMTP-Server aus Sicherheits- oder Funktionalitätsgründen nur auf einer Netzwerk-Schnittstelle laufen lassen (wenn der SMTP-Server zum Beispiel nur auf der internen Netzwerk-Schnittstelle läuft, können nur die Benutzer des lokalen Netzwerks auf SMTP-Dienste zugreifen).

602LAN SUITE enthält auch einen SSL-SMTP-Server, der eine sichere Server-zu-Client-Verbindung bietet. Diesen richten Sie wie einen Standard-SMTP-Server ein. Der Standard-Port für den SSL-SMTP-Server ist 2525. Um SSL-Sicherheit zu nutzen, müssen Sie zuerst ein SSL-Zertifikat erstellen. Weitere Details finden Sie im Abschnitt über die SSL-Konfiguration.

Mails mit dem SMTP-Protokoll empfangen

Das SMTP-Protokoll geht davon aus, dass der SMTP-Server, für den Mails geliefert werden, zugänglich ist (er muss laufen und über eine Internet-Verbindung verfügen). Wenn Ihr 602LAN SUITE SMTP-Server nicht jederzeit mit dem Internet verbunden ist, weil Sie keine permanente Internet-Verbindung verwenden, gibt es zwei Möglichkeiten:

- **Ihr Internetanbieter unterstützt SMTP-Spooling:** Der SMTP-Server Ihres Internetanbieters sieht, dass Ihr 602LAN SUITE SMTP-Server nicht zugänglich ist und bewahrt auszuliefernde Mails in einer SMTP-Warteschlange auf, bis Ihr Server wieder zugänglich ist.

- **Ihr Internetanbieter unterstützt SMTP-Spooling nicht:** Der SMTP-Server Ihres Internetanbieters sieht, dass Ihr 602LAN SUITE SMTP-Server nicht zugänglich ist und bewahrt auszuliefernde Mails in einem POP3-Postfach auf, dass Ihr Internetanbieter für Sie eingerichtet hat.

Die Verarbeitungsmethode für Mails wählen

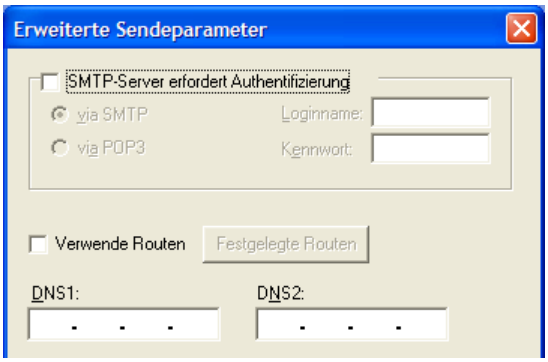
Postversand über den SMTP-Server des Providers

Die einfachste Situation für das Ausliefern von Mails ist die Weitergabe der Mails an den SMTP-Server Ihres Internetanbieters. Geben Sie in diesem Fall den SMTP-Server des Internetanbieters an, entweder mit seinem Namen oder als IP-Adresse und aktivieren Sie "Postversand über den SMTP-Server des Providers".

HINWEIS: Wir empfehlen diese Option des Mail-Versands, wenn Sie eine Einwahlverbindung verwenden, da die Verbindung des Internetanbieters in der Regel wesentlich schneller ist.

Postversand direkt an das Internet mit Hilfe von DNS

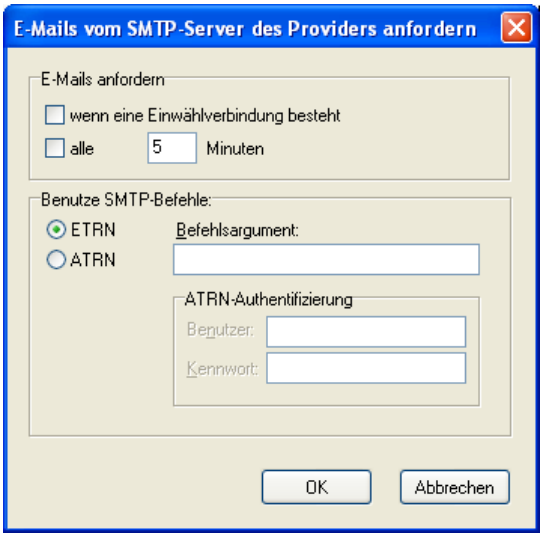
Die Standardmethode, um Mails weiterzuleiten, verwendet den DNS-Dienst (Domain Name Service), um MX-Eintrags-Informationen darüber, wohin eine Mail an eine bestimmte Domäne weiterzuleiten ist, abzurufen. DNS wertet diese Anforderung aus und leitet sie an den nächsten DNS-Server weiter. Dieser Vorgang wird so lange wiederholt, bis der passende MX-Eintrag gefunden ist, der die Zieladresse enthält. Deaktivieren Sie die Option "Postversand über SMTP-Server des Providers" und geben Sie unter "Erweiterte Sendeparameter" in die Eingabefelder "DNS1" und "DNS2" die IP-Adressen von bis zu zwei DNS-Servern an. Diese bekommen Sie von Ihrem Internetanbieter zugewiesen.



HINWEIS: Wir empfehlen, diese Option zu verwenden, wenn Sie eine permanente Internetverbindung verwenden.

Mails vom SMTP-Server des Providers anfordern

Wenn Ihr Internetanbieter Spooling-Dienste anbietet, können Sie Mails von seinem SMTP-Server einsammeln, auch wenn Sie keine permanente Internetverbindung verwenden. Manche Internetanbieter unterstützen ETRN oder ATRN als Anforderung zum Mail-Einsammeln. Wenn Ihr Internetanbieter SMTP-Spooling unterstützt, klicken Sie die Schaltfläche "Mails vom SMTP-Server des Providers anfordern".



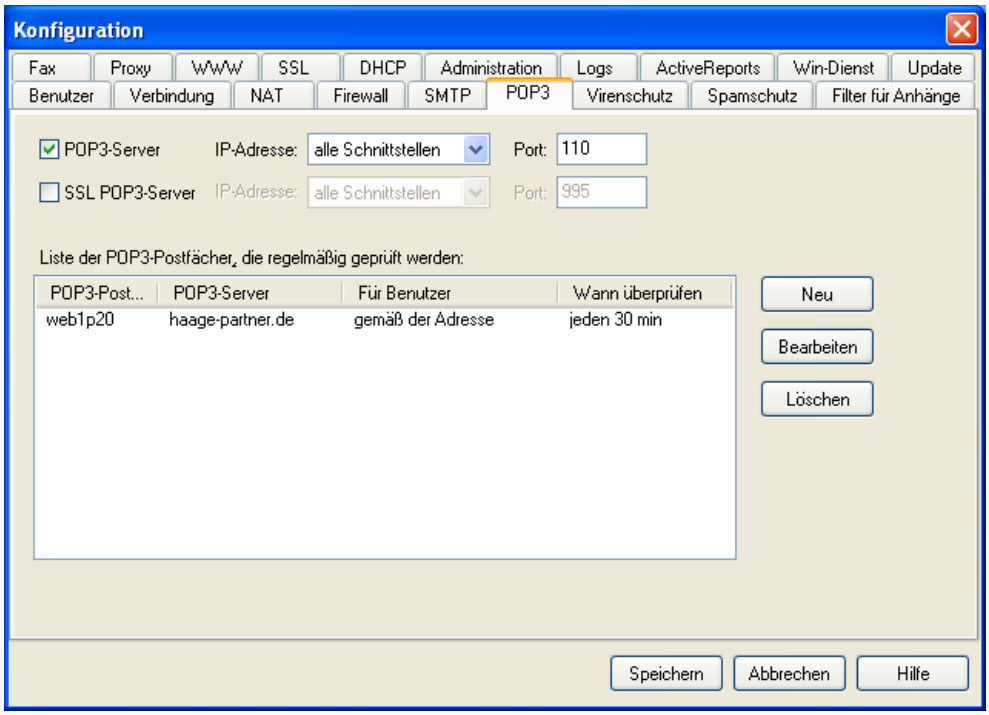
ETRN
ETRN (Extended TURN) ist ein ESMTP-Befehl (zuerst in RFC 1985 definiert) mit dem ein Client mit einer statischen IP-Adresse (602LAN SUITE) den Server (den SMTP-Server Ihres Internetanbieters) dazu auffordert, mit Hilfe einer neuen ESMTP-Verbindung wartende Mails auszuliefern. Bitte fragen Sie Ihren Internetanbieter (Provider) nach den korrekten Argumenten für den ETRN-Befehl.

ATRN
ATRN (Authenticated TURN), auch als On-Demand Mail Relay (ODMR) bekannt, ist ein Mail-Dienst, der einem Client mit einer beliebigen Internetverbindung mit dynamischer IP-Adresse (602LAN SUITE) erlaubt, einen Internetanbieter zu kontaktieren, sich zu authentifizieren und Mails anzufordern. Die Details über ODMR können in RFC 2645 gefunden werden. ATRN benötigt Authentifizierung mit Benutzernamen und Kennwort beim entfernten Server. Der Parameter ist gewöhnlich der Domänenname. Bitte erfragen Sie das korrekte Format des ATRN-Befehls bei Ihrem Internetanbieter.

Mails anfordern
Hier können Sie einrichten, wann Mails angefordert werden. Wählen Sie eines der beiden Auswahlfelder: "Wenn eine Einwahlverbindung besteht" oder "Alle x Minuten". Gemäß dieser Einstellung wird 602LAN SUITE den ETRN- oder den ATRN-Befehl zum Einsammeln der Mails an den Internetanbieter senden und das Mail-Einsammeln beginnen.

POP3-Server-Einstellungen

Post Office Protocol 3 (POP3) ist der Name des Protokolls zum Einsammeln der Mails von Postfächern im Internet. Im Register "POP3" können Sie angeben, von welchen POP3-Postfächern 602LAN SUITE Mails einsammeln und verteilen soll. Indem Sie den POP3-Server aktivieren, können Sie 602LAN SUITE-Benutzern über POP3 Zugang zu Ihren Postfächern geben. Sie können Regeln definieren, von welchen Internet-POP3-Postfächern Mails eingesammelt und an 602LAN SUITE-Benutzerpostfächer ausgeliefert werden.



POP3- oder SSL-POP3-Server einschalten

Benutzen Sie den Schalter "POP3-Server" um den integrierten POP3-Server ein- oder auszuschalten. Sie können die IP-Schnittstelle wählen, auf der dieser Dienst arbeiten soll. Standardmäßig sind alle lokalen Netzwerkschnittstellen angewählt und die Portadresse ist 110. Sie können mit Hilfe des Ausklappmenüs eine IP-Schnittstelle auswählen.

602LAN SUITE enthält auch einen SSL-POP3-Server, der sichere Server-zu-Client-Verbindungen bietet. Richten Sie den SSL-POP3-Server wie den Standard-POP3-Server ein. Der Standard-Port für den SSL-POP3-Server ist 995. Um SSL-Sicherheit zu nutzen, müssen Sie zuerst ein SSL-Zertifikat erstellen. Weitere Details finden Sie im Abschnitt über die SSL-Konfiguration.

Liste der POP3-Postfächer

Klicken Sie "Neu" um eine neue Regel zum Einsammeln eines POP3-Postfaches zu definieren und geben Sie die POP3-Zugangsinformationen in die Eingabefelder ein. Wenn Sie eine Regel löschen möchten, wählen Sie diese aus und klicken Sie auf "Löschen". Mit "Bearbeiten" können Sie eine bestehende Regel ändern.

Ein Postfach im Internet wird durch die Adresse des Mailservers (als Name oder IP-Adresse) und den Namen des Benutzers identifiziert, der Zugang wird über ein Kennwort gewährt, das dem Benutzerpostfach beim Erstellen zugewiesen wurde. Geben Sie die entsprechenden Angaben in die Eingabefelder ein:

- POP3-Server (Computer-Adresse, z.B. 192.168.1.1)
- Login-Name (Benutzername)
- Kennwort
- APOP-Loginmethode

Die APOP-Loginmethode bietet zusätzlichen Schutz für den Computer, der das Internet-Postfach verwaltet. Es wird kein Kennwort gesendet. Der Server sendet nur eine zufällige Zeichenkette, womit der Client einen

Abdruck des Kennwortes erstellt, den er zum Überprüfen an den Server zurückschickt. Fragen Sie Ihren Internetanbieter, ob er diese Login-Methode unterstützt.

Mails weiterleiten

Mails von einem POP3-Postfach können automatisch eingesammelt und in ein lokales Benutzerpostfach einsortiert werden:

- Gemäß der Adresse
- An einen bestimmten Benutzer

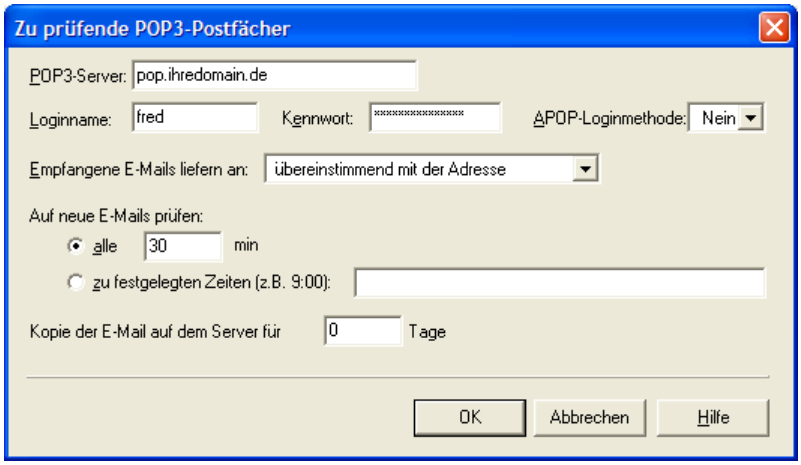
Um einem 602LAN SUITE-Benutzer ein POP3-Postfach zuzuweisen, wählen Sie bei "Empfangene Mails liefern" den entsprechenden lokalen Benutzer aus. Wenn über einen POP mehrere Mailadressen ankommen, dann können diese auch auf verschieden 602LAN SUITE-Benutzer, in Abhängigkeit von deren Namen bzw. Alias, verteilt werden. Wählen Sie dann den Punkt „Gemäß der Adresse“.

HINWEIS: Sie können ankommende Mails auch an mehrere 602LAN SUITE-Benutzer weiterleiten. Im Register „Benutzer“ tragen Sie dann die entsprechende Empfängeradresse (z.B. support@firma.de) als Alias bei allen Benutzern ein, die diese Mails erhalten sollen.

Postfach-Einsammel-Intervall

Mails können von POP3-Postfächern zu festgelegten Zeiten oder in einem bestimmten Intervall eingesammelt werden:

- **Alle x Minuten:** Geben Sie das Zeitintervall für das Einsammeln der Mails des POP3-Postfaches ein.
- **Zu festgelegten Zeiten:** Geben Sie die Zeiten im 24-Stunden-Format an, wann die Mails des POP3-Postfaches eingesammelt werden sollen. Trennen Sie mehrere Zeitangaben mit Kommas.



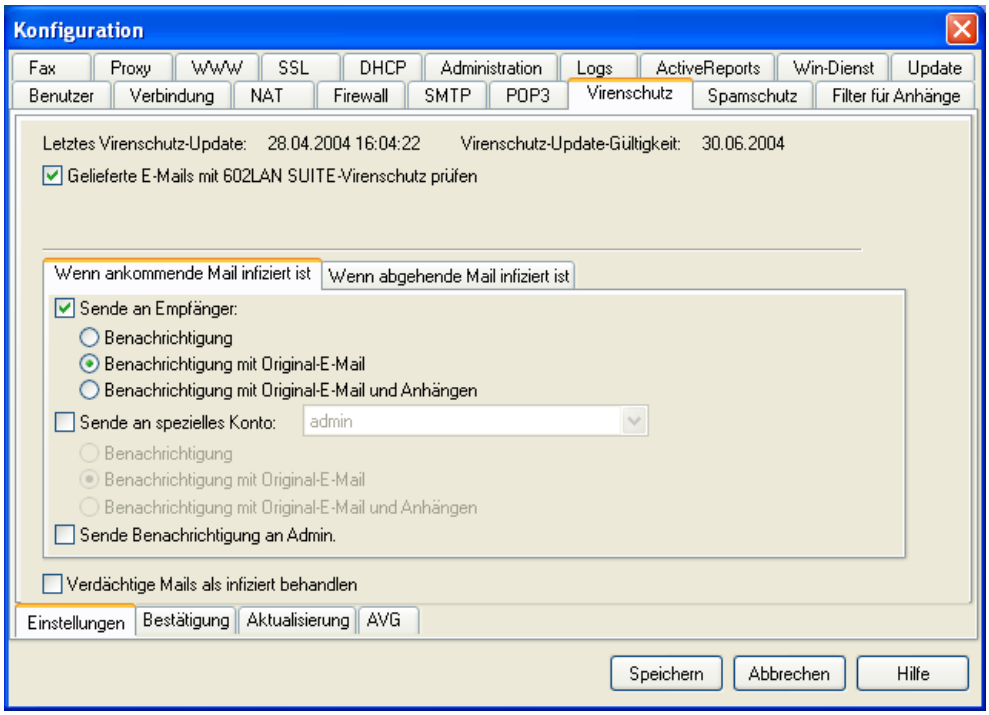
HINWEIS: Dies Intervall kann genauer eingestellt werden, wenn Sie im Register "Verbindung" zusätzlich eine globale Zeitbeschränkung verwenden.

Kopie der Mails auf dem POP3-Server hinterlassen

Alle Mails, die von einem POP3-Server mit 602LAN SUITE eingesammelt werden, werden vom POP3-Server gelöscht. Wenn Sie die Mails auf dem POP3-Server belassen wollen, geben Sie die Anzahl der gewünschten Tage ein.

Virenschutz konfigurieren

602LAN SUITE Antivirus-Edition kann Mails mit Hilfe der BitDefender-Technologie auf Viren prüfen. Alle eingehenden Mails werden mitsamt eventuellen Anhängen auf Viren und Würmer geprüft, bevor Sie in die Benutzer-Postfächer gelangen. Die BitDefender-Engine wurde von den ICSA Labs und den West Coast Labs zertifiziert, erhielt mehrere VB 100%-Auszeichnungen und bietet eine außergewöhnlich hohe Scangeschwindigkeit und Erkennungsrate.



Die enge Integration mit der BitDefender Antivirus-Software bietet ein erweitertes Viren-Warnsystem. Alle infizierten Teile einer Mail können automatisch entfernt werden. Dem Empfänger kann eine Benachrichtigung gesendet und die komplette Mail kann für den Systemverwalter an ein spezielles Mail-Konto geliefert werden. Um das Überprüfen von Mails einzuschalten, aktivieren Sie die Option "E-Mails mit 602LAN SUITE-Virenschutz prüfen" im Register "Virenschutz". Sie haben mehrere Optionen, um zu bestimmen was beim Entdecken infizierter Mails geschehen soll:

- **Sende an Empfänger**
  - Benachrichtigung
  - Benachrichtigung mit Original-Mail
  - Benachrichtigung mit Original-Mail und Anhängen
- **Sende an spezielles Konto** – Wählen Sie ein Konto aus dem Ausklappmenü.
  - Benachrichtigung
  - Benachrichtigung mit Original-Mail
  - Benachrichtigung mit Original-Mail und Anhängen
- **Sende Benachrichtigung an Administrator**

Wenn eine Mail als verdächtig markiert wird, können Sie sie als infiziert behandeln, indem Sie die Option „**Verdächtige Mails als infiziert behandeln“** einschalten. Wenn diese Option nicht aktiviert ist, behandelt 602LAN SUITE verdächtige Mails als **nicht infiziert**.

Zertifizierung – Alle geprüften Mails können mit einer Zertifizierungsmarkierung versehen werden. In diesem Register können Sie die Zertifizierung einschalten und den Zertifizierungstext festlegen.

Aktualisierung – Täglich erscheinen neue Viren. Um Ihren Virenschutz auf dem aktuellen Stand zu halten, empfehlen wir die Option "Automatische Virenschutz-Updates einschalten" zu aktivieren. Sie können ein Zeitintervall in Stunden angeben, wie oft die Viren-Datenbank aktualisiert werden soll. Wenn Sie die Viren-Datenbank manuell aktualisieren möchten, klicken Sie auf den Schalter "Jetzt aktualisieren".

AVG - 602LAN SUITE unterstützt auch die Virenschutz-Software AVG von Grisoft, Inc. Wenn Sie AVG auf diesem Computer installiert haben und es verwenden möchten, um eingehende Mails zu prüfen, aktivieren Sie die Option "Ankommende Mails mit AVG-Antivirus prüfen".

HINWEIS: 602LAN SUITE unterstützt das gleichzeitige Überprüfen mit 602LAN SUITE-Antivirus und AVG.

Mailclient konfigurieren

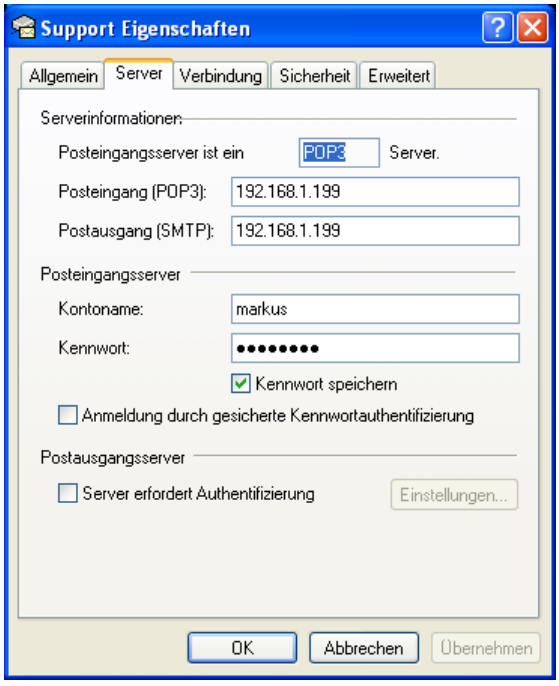
602LAN SUITE unterstützt zwei Arten des Sendens und Empfangens von Mails:

- Die Verwendung eines POP3-/SMTP-fähigen E-Mail-Programms eines Drittanbieters wie Microsoft Outlook, Outlook Express, Eudora, KMail, Evolution, Mozilla, Netscape Messenger usw.
- Der 602LAN SUITE Webmail-Client

Hier beschreiben wir die Einrichtung des Mail-Programms anhand von Microsoft® Outlook und Microsoft® Outlook Express. Diese Anweisungen können auch als Wegweiser für das Einrichten anderer Mail-Clients verwendet werden.

Microsoft® Outlook Express 6.x einrichten

1. Öffnen Sie Outlook Express.
2. Wählen Sie den Menüpunkt „Extras“ und dort den Punkt „Konten“. Es öffnet sich ein Dialog. Dort wählen Sie „Hinzufügen“ und „E-Mail“.
3. Geben Sie Ihren in das Feld "Ihr Name" Ihren vollständigen Namen an und klicken Sie "Weiter".
4. Wählen Sie "Ich habe bereits eine Mail-Adresse" und geben Sie in das Feld "E-Mail-Adresse" Ihre Mail-Adresse ein und klicken Sie auf "Weiter".
5. Geben Sie als Posteingangsserver und als Postausgangsserver die IP-Adresse des 602LAN SUITE Servers an (möglicherweise 192.168.1.1). Klicken Sie dann auf "Weiter".
6. Geben Sie im Feld "Kontoname" den Benutzernamen des betreffenden 602LAN SUITE-Benutzers ein.
7. Geben Sie im Feld "Kennwort" das Kennwort des Benutzers ein.
8. Stellen Sie sicher, dass die Option "Anmeldung durch gesicherte Kennwortauthentifizierung (SPA)" nicht angewählt ist.
9. Klicken Sie "Weiter".
10. Klicken Sie "Fertig stellen".



Microsoft® Outlook 2002 einrichten

1. Öffnen Sie Outlook.
2. Wählen Sie "Extras/Konten" aus dem Menü.
3. Wählen Sie "Mail/Hinzufügen" und klicken Sie "Weiter".
4. Geben Sie im Feld "Mail-Adresse" Ihre Mail-Adresse ein. Klicken Sie dann auf "Weiter".
5. Wählen Sie als Posteingangsserver "POP3".
6. Geben Sie als Posteingangsserver die IP-Adresse des 602LAN SUITE-Servers an (möglicherweise 192.168.1.1).

7. Geben Sie als Postausgangsserver die IP-Adresse des 602LAN SUITE-Servers an (möglicherweise 192.168.1.1). Klicken Sie dann auf "Weiter".
8. Geben Sie im Feld "Kontoname" den Benutzernamen des betreffenden 602LAN SUITE-Benutzers ein.
9. Geben Sie im Feld "Kennwort" das Kennwort des Benutzers ein.
10. Stellen Sie sicher, dass die Option "Anmeldung durch gesicherte Kennwortauthentifizierung (SPA)" nicht angewählt ist.
11. Klicken Sie "Weiter".
12. Wählen Sie "Über das lokale Netzwerk (LAN) verbinden", wenn Sie vom lokalen Netzwerk auf Ihr 602LAN SUITE POP3-Postfach zugreifen. Andernfalls geben Sie an, wie die Internet-Verbindung hergestellt werden soll. Klicken Sie "Weiter".
13. Klicken Sie "Fertig stellen".

Auf den Webmail-Client zugreifen

602LAN SUITE Web Mail - Mozilla
Datei Bearbeiten Ansicht Gehe Lesezeichen Tools Fenster Hilfe
http://127.0.0.1/mail
602 LAN SUITE
E-mail • Fax • Web
Anti-spam • Anti-virus
Proxy • Firewall/NAT
Bitte melden Sie sich an:
Benutzername:
Kennwort:
Anmelden
Benutzername und Kennwort merken
Wichtig! Denken Sie daran, sich abzumelden.
Denken Sie zu Ihrer Sicherheit immer daran, auf "Abmelden" zu klicken, wenn Sie fertig sind.
© Software602, Inc

Starten Sie einen Webbrowser und geben Sie die IP-Adresse oder den Namen des Computers an, auf dem 602LAN SUITE läuft (z.B. http://192.168.1.1/mail oder http://www.ihre-firma.de/mail):

1. Geben Sie Ihren Benutzernamen an. Beim Benutzernamen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
2. Geben Sie Ihr Kennwort ein. Beim Kennwort wird nicht zwischen Groß- und Kleinschreibung unterschieden.
3. Klicken Sie auf "Anmelden".

HINWEIS: Für die Verwendung des Webmail-Clients muss der 602LAN SUITE-Webserver aktiviert sein!

HINWEIS: Wenn der SSL-WWW-Server aktiviert ist, können Sie statt mit http (HTTP-Protokoll) auch mit https (SSL-geschütztes HTTP-Protokoll) auf dem Webmail-Client zugreifen (beispielsweise https://192.168.1.1/mail).

Webserver konfigurieren

WWW-Konfiguration

Aktivieren Sie "WWW-Server", wenn Sie die Funktionalität des eingebauten WWW-Servers verwenden möchten. Sie können unter "WWW-IP-Adresse" eine IP-Schnittstelle auswählen, auf der der Server arbeitet. Standardmäßig verwendet der Webserver alle lokalen Netzwerk-Schnittstellen, doch Sie können eine spezifische Schnittstelle auswählen. Zudem können Sie im Feld "WWW-Port" angeben, welcher Port für den Webserver verwendet werden soll (standardmäßig 80).

HINWEIS: Wenn Sie einen anderen Webserver als den in 602LAN SUITE eingebauten Webserver verwenden möchten, müssen Sie den eingebauten Webserver ausschalten oder auf einem anderen Port (z.B. 8080) laufen lassen. So können Sie die Fernadministration über WWW nutzen, ohne einen bereits laufenden Webserver im Betrieb zu stören.

Geben Sie Folgendes an, um den WWW-Server zu nutzen:

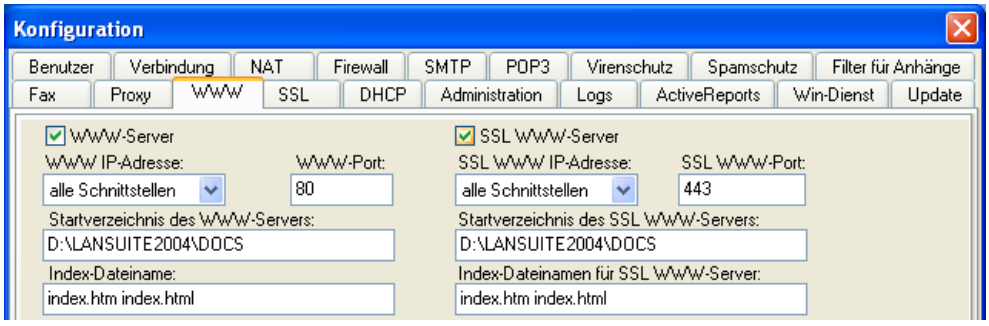
- **Startverzeichnis des WWW-Servers** - Pfad zum Wurzelverzeichnis (Root-Verzeichnis) des WWW-Servers.
- **Index-Dateiname** - Dateiname, der für die Indexseite verwendet wird. Sie können mehrere Namen mit Leerzeichen voneinander trennen, z.B.: "index.html index.htm index.php".
- **Skriptverzeichnis** - Verzeichnis für CGI- oder FastCGI-Skripte.
- **Umgebungsvariablen für Skripte** – Verzeichnis für Umgebungsvariablen für Skripte.
- **Benutzer-Startverzeichnis** - Das Verzeichnis, in das persönliche Benutzer-Webseiten platziert werden.

Sobald dieses Verzeichnis festgelegt ist, legt 602LAN SUITE automatisch für jeden neu erstellten Benutzer in diesem Startverzeichnis ein Unterverzeichnis mit dessen Name an. Benutzer-Webseiten können mit http://computername/~benutzername aufgerufen werden.

Ein Benutzer kann sein Home-Verzeichnis auf folgende Arten aktualisieren:

- Auf dem Computer, auf dem 602LAN SUITE läuft, Dateien in den entsprechenden Benutzer-WWW-Ordner kopieren.
- Die Webseiten nach Anmelden mit Benutzername und Kennwort mittels Netscape Navigator oder Mozilla mittels HTTP-Protokoll hoch laden.
- Die Dateien mittels FTP-Protokoll hochladen – In diesem Fall müssen die WWW-Ordner als Unterverzeichnisse des globalen WWW-Startverzeichnisses erstellt werden ("Startverzeichnis des WWW-Servers").

602LAN SUITE enthält auch einen SSL-WWW-Server, der sichere Server-zu-Client-Verbindungen bietet. Richten Sie den SSL-WWW-Server wie den Standard-WWW-Server ein. Der Standard-Port für den SSL-WWW-Server ist 443. Sie müssen ein Zertifikat erstellen, das Sie entweder selbst signieren oder von einer Certificate Authority wie VeriSign, Thawte oder Comodo zertifizieren lassen. Wenn Sie ein SSL-Zertifikat kaufen, wird dies von allen Browsern global erkannt und Ihre Webseite automatisch als vertrauenswürdig eingestuft. Bei einem selbst signierten Zertifikat wird der Webbrowser melden, dass das Zertifikat nicht erkannt wurde. Der Zugriff auf die Webseite ist dennoch SSL-gesichert.



Benutzer-Ordner verwenden

Jeder Benutzer hat ein eigenes Verzeichnis (Home) auf dem WWW-Server, in dem er Informationen veröffentlichen kann. Die Benutzer-Verzeichnisse können von einem Webbrowser mit

http://computername/~benutzername aufgerufen werden. "computername" ist der Name des Computers, auf dem 602LAN SUITE läuft, und "benutzername" der Name des 602LAN SUITE-Benutzers, auf dessen persönliche Webseite zugegriffen werden soll.

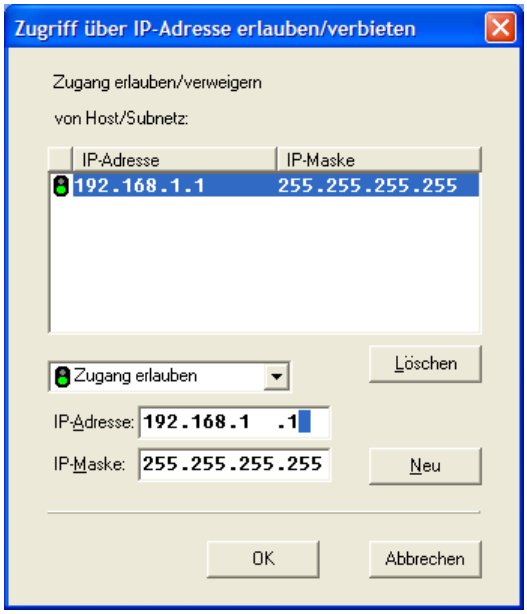
Benutzer können Ihre Seiten wie folgt aktualisieren:

- Dateien direkt auf den Dateiserver in das Benutzer-Verzeichnis kopieren.
- Dateien mit Netscape Navigator oder Mozilla mittels HTTP nach Anmelden mit Benutzername und Kennwort hochladen.
- Mit einem FTP-Client auf das Benutzerverzeichnis zugreifen. Geben Sie den Computernamen, den Benutzernamen und das Kennwort an.

Wenn der Benutzer kein Administrator ist, darf er nur auf sein Home-Verzeichnis zugreifen.
Wenn der Benutzer Administrator ist, darf er auf das Startverzeichnis des WWW-Servers und damit auf alle Benutzerverzeichnisse zugreifen.

Zugriffsfilter

Wenn Sie die Option "IP-Filter für Zugang zum WWW-Server" aktivieren, definiert der WWW- & SSL-WWW-IP-Filter anhand von Regeln den Zugang zum WWW-Server. Die IP-Filter-Regeln werden von oben nach unten überprüft. Jede nachfolgende Regel überstimmt gegebenenfalls die vorhergehenden Regeln. Geben Sie die IP-Adresse und die Maske des Computers oder Netzwerks an, das die Anforderung sendet, in die Felder "IP-Adresse" und "IP-Maske" ein. Definieren Sie dann, ob dem betreffenden Computer oder Netzwerk der Zugang erlaubt oder verweigert wird! ROT bedeutet Zugang verweigern, GRÜN bedeutet Zugang erlauben.



Verzeichnis durchsuchen

Wenn Sie die Option "Verzeichnis durchsuchen" aktivieren, erlaubt der Webserver Besuchern den Inhalt von Verzeichnissen zu durchsuchen, die keine Index-Seite haben. Diese Funktion stellt unter Umständen ein Sicherheitsrisiko dar, da man gegebenenfalls auf Inhalte zugreifen kann, die man normalerweise nicht sehen würde.

Webserver-Inhalt aktualisieren

Sie können den Inhalt des Webservers auf zwei Arten aktualisieren:

- Lokal
- Von einem entfernten Computer mittels FTP

Aktualisieren vom lokalen Server aus

Aktualisieren Sie Ihre Webseiten, indem Sie die aktualisierten Dateien in das Startverzeichnis des WWW-Servers kopieren. Standardmäßig ist das Startverzeichnis das "DOCS"-Verzeichnis im 602LAN SUITE-Ordner. Sie können es im Register "WWW" konfigurieren.

Von einem entfernten Computer mittels FTP aktualisieren

Die bekannteste Art, um den Inhalt eines Webservers zu aktualisieren, ist das Übertragen der aktualisierten Dateien mit Hilfe des FTP-Protokolls.

Dafür gibt es ein paar Voraussetzungen:

- Unter "Administration" muss die Option "Erlaube Updates des WWW-Servers mittels FTP" aktiviert sein.
- Sie müssen ein Administrator sein, um auf das Startverzeichnis des WWW-Servers zuzugreifen. Ein Standard-Benutzer kann nur auf sein eigenes Verzeichnis zugreifen.

Verwenden Sie ein FTP-Programm, um mit dem 602LAN SUITE-Server Verbindung aufzunehmen. Administratoren werden mit dem Startverzeichnis des WWW-Servers verbunden, Standard-Benutzer mit Ihrem Home-Verzeichnis. Bitte lesen Sie die Anleitung Ihres FTP-Clients für Upload-Anweisungen. Internet Explorer kann als FTP-Client verwendet werden.

Sie können MSIE wie folgt verwenden:

1. Tippen Sie "ftp://ihrserver.de", wobei Sie "ihrserver.de" durch den Namen oder die IP-Adresse Ihres 602LAN SUITE-Servers ersetzen.
2. Sie werden aufgefordert, sich mit Benutzername und Kennwort anzumelden. Anonymer Zugang wird nicht unterstützt.
3. Als Administrator werden Sie nun mit dem Startverzeichnis des WWW-Servers verbunden, als regulärer Benutzer mit Ihrem persönlichen Home-Verzeichnis.
4. Benutzen Sie die Standard-Befehle "Kopieren" und "Einfügen", um Dateien zwischen Ihrem Computer und dem FTP-Server zu übertragen.

Einen SSL-Webserver einrichten

Aktivieren Sie "SSL WWW-Server", um den SSL-Webserver zu verwenden. Sie müssen ein SSL-Zertifikat erstellt haben, um die Änderungen speichern zu können. Details dazu finden Sie im Abschnitt zur SSL-Konfiguration. Der SSL-Webserver hat seine eigenen konfigurierbaren Parameter. Diese sind standardmäßig mit denen des regulären Webservers identisch. Dies ermöglicht Ihnen, Dokumente, die der SSL-Webserver lokal oder im Internet anbieten soll, in einem anderen Verzeichnis abzulegen.

Der SSL-Webserver bietet die folgenden Vorteile:

- Sie können den Webmail-Client von 602LAN SUITE über eine sichere SSL-Verbindung verwenden, damit die Mails sicher übertragen werden. Beispiel: https://ihrserver/mail.
- Sie können die Fernadministration Ihres 602LAN SUITE WWW-Servers mittels Webbrowser mit SSL-Verschlüsselung absichern. Beispiel: https://ihrserver/admin

FastCGI-Anwendungen

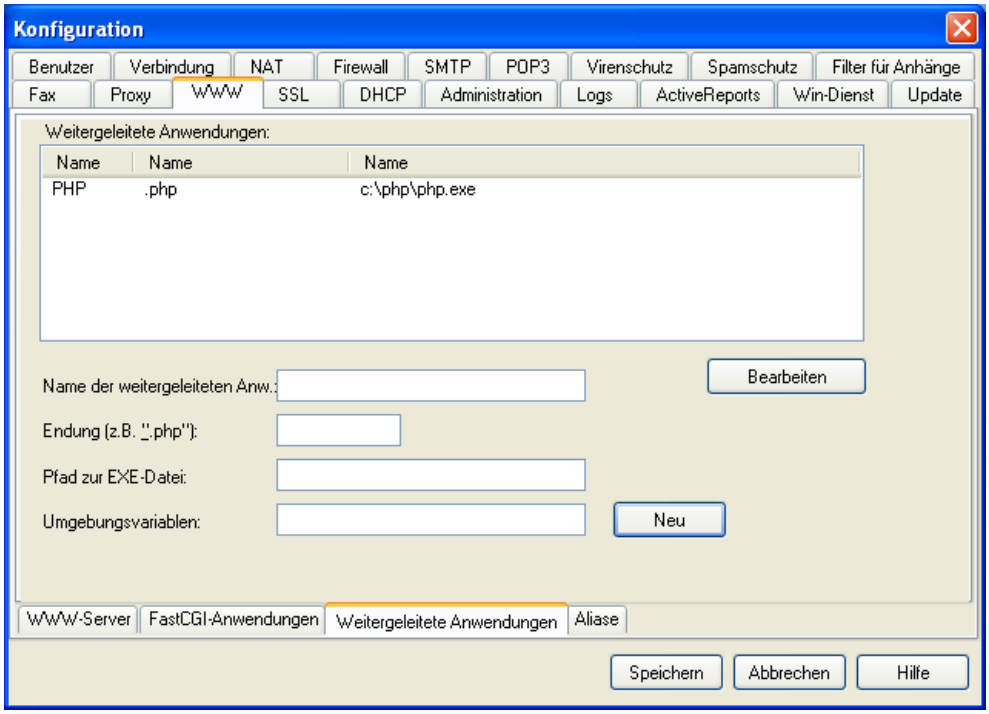
Um eine FastCGI-Anwendung zu nutzen, registrierten Sie sie, indem Sie die folgenden Werte definieren:

- **FastCGI-Anwendungsname** – Anwendungsname, der in der Liste angezeigt wird.
- **Rolle** – Eine FastCGI-Anwendung kann verschiedene Typen von Anforderungen bearbeiten (sie kann mehrere Rollen haben). Hier müssen Sie angeben, welche Rolle Sie Ihrer FastCGI-Anwendung geben möchten. Wenn Sie eine nicht speziell programmierte Anwendung verwenden, sollte die Rolle "1" sein (die Anwendung liefert eine HTML-Seite, die zum angegebenen Pfad passt). Die folgenden Regeln sind vordefiniert: Responder, Authorizer und Filter.
- **Ort (URL)** – Ort (URL), die der Benutzer im WWW-Browser angibt, um diese FastCGI-Anwendung zu starten.
- **Verbindung (adresse:port)** – Es ist erforderlich anzugeben, auf welchem Computer (IP-Adresse) und welchem Port die FastCGI-Anwendung läuft. Wenn die Anwendung auf dem lokalen Computer läuft, können Sie nur die Portnummer angeben oder "localhost:port".
- **Pfad zur EXE-Datei** – Wenn sich die ausführbare Datei für die FastCGI-Anwendung auf diesem Computer befindet, kann der WWW-Server diese Datei beim Start öffnen, sodass er gleich bereit ist, eine Anforderung zu bearbeiten.
- **Umgebungsvariablen** – Die FastCGI-Anwendung erhält vom WWW-Server Informationen über die aufgebaute Verbindung und den Server-Typ. Hier können Sie zu übergebende Umgebungsvariablen in folgendem Format definieren: variablenname=wert. Trennen Sie mehrere Variablen mit Semikolons voneinander.

Weitere Informationen zu FastCGI finden Sie auf der WWW-Seite: http://www.fastcgi.com.

Weitergeleitete Anwendungen (Mapped Applications)

Wenn der WWW-Server Dateien mit einer Endung findet, die Sie für eine weitergeleitete Anwendung im Feld "Endung" angegeben haben, startet er die Anwendung, die Sie im Feld "Pfad zur EXE-Datei" angegeben haben. Um eine weitergeleitete Anwendung zu verwenden, registrierten Sie die Anwendung mit den folgenden Parametern:



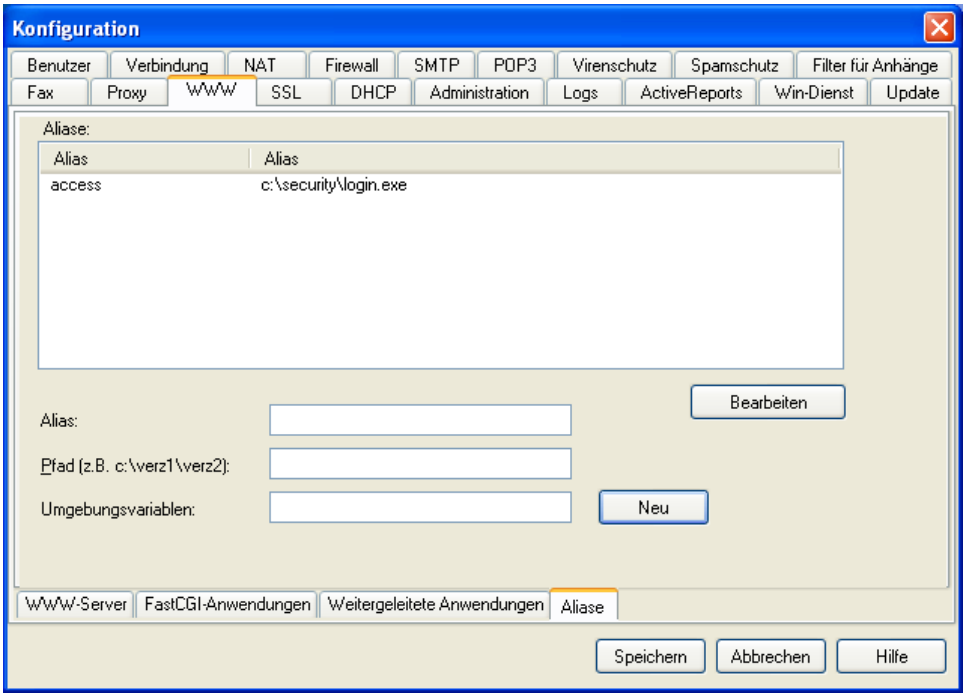
- **Name der weitergeleiteten Anwendung** – Anwendungsname, der in der Liste angezeigt wird.
- **Endung** – Geben Sie die Datei-Endung an (z.B. ".php").

- **Pfad zur EXE-Datei** – Geben Sie den vollen Pfad zur EXE-Datei der Anwendung an. Der WWW-Server wird die Anwendung starten, wenn eine Datei angefordert wird, deren Dateiname mit der angegebenen Endung endet.
- **Umgebungsvariablen** – Sie können weitergeleitete Anwendungen mit verschiedenen Parametern laufen lassen. Trennen Sie mehrere Parameter mit Semikolons.

Aliase

Um einen Alias auf dem Webserver zu verwenden, definieren Sie ihn durch die folgenden Angaben:

- **Pfad** – Definieren Sie den lokalen Pfad, für den Sie einen Alias erstellen möchten.
- **Alias** – Definieren Sie den Alias, wie er vom WWW-Server aus zugänglich sein soll.
- **Umgebungsvariablen** – Es ist möglich, in eine URL-Anforderung eine Anwendung (EXE-Datei) mit einzuschließen. Trennen Sie mehrere Parameter durch Semikolons.



Faxserver konfigurieren

Das Register "Fax" wird verwendet, um Parameter zu setzen, die das Senden und Empfangen von Faxen steuern. Faxe können mit Hilfe eines Faxmodems versendet werden. Dieses Register hat zwei Unterregister:

- **Faxserver:** Für allgemeine Einstellungen.
- **TAPI:** Um das TAPI-Gerät (Faxmodem) einzurichten.

Allgemein

In diesem Register definieren Sie die Faxmethode und die Arbeitsintervalle.

Fax-Identifikation

Geben Sie in das Feld "Fax-Identifikation" eine Zeichenkette an, die den Faxabsender identifiziert. Diese Information wird während der ersten Phase der Übermittlung an das entfernte Faxgerät übertragen und erlaubt dem Empfänger, Sie zu identifizieren. Diese Identifikation sollte Ihre Faxnummer enthalten.

Empfangene Faxe ausdrucken

Wenn Sie empfangende Faxe ausdrucken möchten, wählen Sie aus dem Ausklappmenü "Empfangene Faxe drucken über" einen Drucker aus.

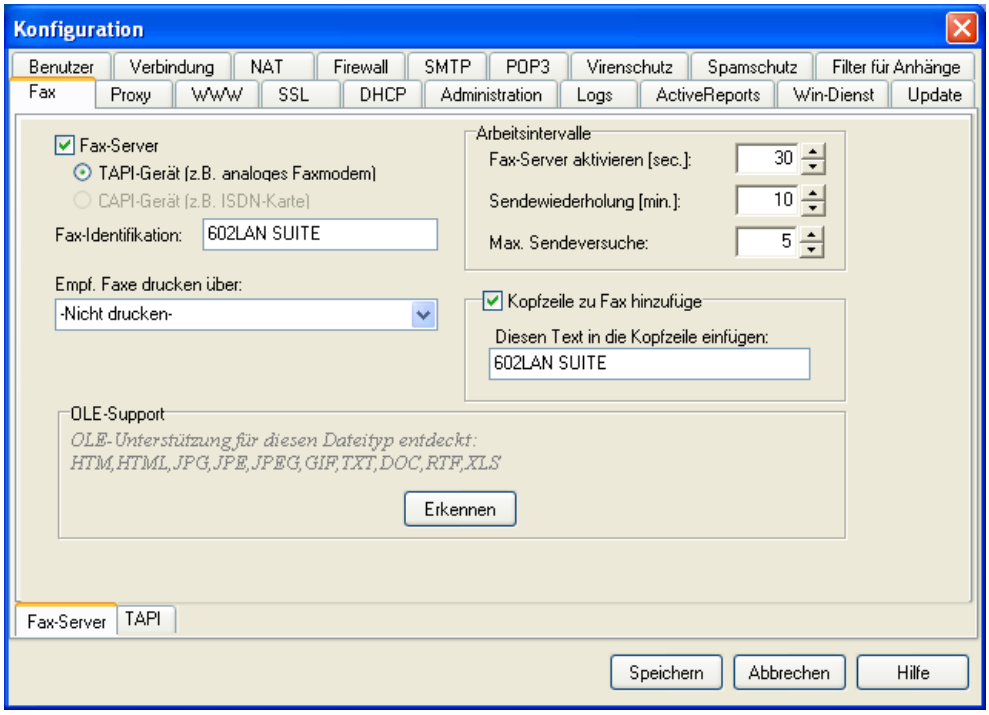
Arbeitsintervalle

In diesem Bereich können Sie das Zeitintervall zum Handhaben der Faxkommunikation einstellen:

- **Faxserver aktivieren:** Der Faxserver prüft die Fax-Warteschlange alle x Sekunden und versucht alle wartenden Faxe zu versenden.
- **Sendewiederholung:** Verläuft ein Sendeversuch nicht erfolgreich, wird der Faxserver nach x Minuten erneut versuchen, das/die betreffende(n) Fax(e) zu versenden.
- **Max. Anzahl Sendeversuche:** Definiert die Anzahl der Versuche, Faxe zu versenden. Der erste Sendeversuch beinhaltet 4 Einwahlversuche und der darauf folgende 2 Einwahlversuche.

Kopfzeile zu Fax hinzufügen

Sie können im Feld "Diesen Text in die Kopfzeile hinzufügen" einen Text eingeben, der als Kopfzeile auf jeder Faxseite mitgesendet wird. Diese Information kann zum Beispiel Ihre Identifikation enthalten.

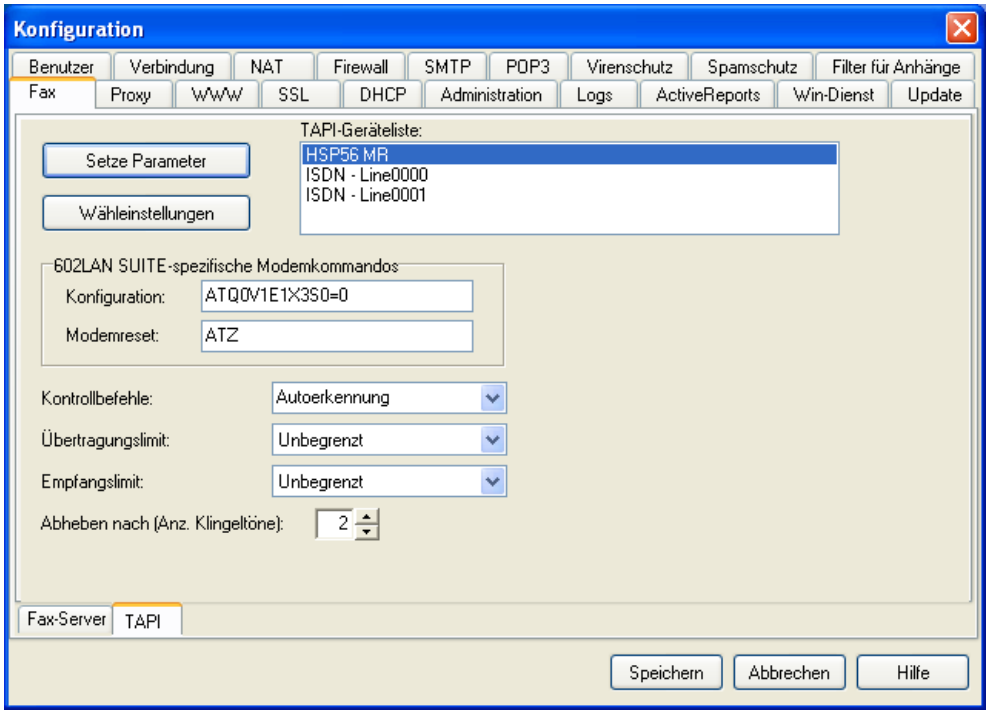


TAPI

Dieses Register setzt die Parameter für das TAPI-Gerät (Faxmodem). In der "TAPI-Geräteliste" werden alle verfügbaren TAPI-Geräte angezeigt.

Parameter und Wähleinstellungen

Die Schaltflächen "Parameter" und "Wähleinstellungen" öffnen Konfigurationsdialoge des Windows-Betriebssystems. Sie können diese Fenster auch aus der Systemsteuerung unter "Telefon- und Modemoptionen" heraus öffnen.



602LAN SUITE-spezifische Modembefehle

- **Konfiguration** – Modembefehl, um Ihr Modem für 602LAN SUITE zu konfigurieren.
- **Modemreset** – Modembefehl, um Ihr Modem zurückzusetzen.

Kontrollbefehle

Faxmodems unterstützen mehrere Befehlssätze für die Faxübertragung. Diese Option erlaubt Ihnen, den entsprechenden Befehlssatz auszuwählen oder die automatische Erkennung einzuschalten.

- **Klasse 1 (Class 1):** Beim ältesten Befehlssatz erledigt der Computer die meisten Faxoperationen. Dieser Befehlssatz wurde zu einem Standard zusammengefasst und ist deshalb in Faxmodems und -programmen häufig implementiert. Der Originalstandard kannte keine Definition, wie ein Modem einen Datenanruf von einem Faxanruf unterscheiden kann. Ältere US Robotics-Modems unterstützen Klasse 1. Klasse 1 und Klasse 2 werden von allen Modems, die auf dem ROCKWELL-Chipsatz basieren, unterstützt.
- **Klasse 2 (Class 2):** Das Faxmodem erledigt bestimmte Kommunikationsoperationen (ein gemeinsames Protokoll mit der Gegenstelle ermitteln, Seiten bestätigen, Verbindung beenden) automatisch oder als Antwort auf einen AT-Befehl. Dieser Befehlssatz wurde nicht zu einem Standard; es handelt sich nur um einen Satz von Empfehlungen, die von manchen Herstellen nicht exakt befolgt werden. Auch hier gibt es keine klare Unterscheidung zwischen Daten- und Faxanrufen. Dieser Befehlssatz wird von vielen Faxmodems unterstützt. Alle ZyXEL-Modems der FW-Serie unterstützen ihn. US Robotics hat diesen Befehlssatz nicht implementiert.
- **Klasse 2.0 (Class 2.0):** Die letzte Version ist dem Klasse 2-Befehlsatz in Bezug auf die Befehlsstruktur und die Arbeitsweise sehr ähnlich. Die Befehle sind kürzer und es wurden einige Extra-Befehle eingeführt, die die Probleme mit Klasse 2 lösen. Dieser Befehlssatz ist voll standardisiert, aber noch nicht weit verbreitet. Seine Beliebtheit steigt jedoch. ZyXEL Elite, ZyXEL 1496, FW 6.12+ und US Robotics unterstützten diesen Standard. ROCKWELL unterstützt ihn nicht.

Übertragungs- und Empfangsgeschwindigkeit begrenzen
Die Eingabefelder "Übertragungslimit" und "Empfangslimit" ermöglichen Ihnen, die maximale Geschwindigkeit der Faxübertragung zu begrenzen und damit an die Leitungsqualität anzupassen. Wählen Sie "unbegrenzte Geschwindigkeit" oder eine Standard-Geschwindigkeit zwischen 2.400 und 14.400 Bit/s aus dem Ausklappmenü.

Abheben nach x Klingelzeichen
Im Eingabefeld "Abheben nach (Anzahl Klingeltöne)" erlaubt Ihnen, die Anzahl der Klingelzeichen anzugeben, nach denen das Faxmodem auf einen eingehenden Faxanruf antworten soll.

Installation des SendFax-Clients

Wenn Sie aus jeder Anwendung heraus direkt über die Druckfunktion Faxe verschicken möchten, ist es erforderlich, dass Sie auf den Client-Computern den SendFax-Client installierten.

1. Laden Sie den SendFax-Client von http://www.software602.de/download.html
2. Starten Sie das Installationsprogramm aus dem Verzeichnis, in das Sie es geladen haben. Folgen Sie den Anweisungen des Installationsprogramms.
3. Nachdem Sie die Lizenzvereinbarung akzeptiert haben, geben Sie im Feld "Name" Ihren Namen und in Feld "Firma" den Namen Ihrer Firma an.
4. Nun geben Sie an, in welches Verzeichnis der SendFax-Client installiert werden soll.
5. Nun werden alle Programmdateien in das Installationsverzeichnis kopiert und ein neuer Druckertreiber eingerichtet.

Fax mit SendFax-Client versenden

Wenn Sie direkt aus einer Anwendung mit Druckfunktion (z.B. MS Word) ein Fax versenden wollen, erstellen oder laden Sie zunächst das Dokument und drucken Sie es dann mit dem "Fax602"-Druckertreiber. Der SendFax-Druckertreiber erstellt ein Fax. Nun erscheint das Fenster der Sendfax-Konfiguration mit der Adressbuch-Seite. Geben Sie dort die Faxnummer des Empfängers an oder wählen Sie einen Eintrag aus dem Adressbuch. Danach wird das Fax an 602LAN SUITE gesendet. Die Schritte im Einzelnen:

1. Sie können jedes Windows-Programm mit Druckfunktion verwenden. Wählen Sie bei der betreffenden Anwendung "Datei/Drucken" aus dem Menü und wählen Sie dann den "Fax602"-Druckertreiber.
2. Nun können Sie einen oder mehrere Empfänger eingeben oder aus der Liste des Adressbuches wählen.
3. Wählen Sie die Seitenlänge und überprüfen Sie die Vorschau, wenn Sie vor dem Senden sehen möchten, wie Ihr Fax aussehen wird.
4. Wählen Sie den oder die Empfänger.
5. Überprüfen Sie die Faxvorschau (wenn Sie diese Option wählten).
6. Klicken Sie auf "Senden", wenn Sie fertig sind.

Fax mittels Mail versenden

Wenn Sie direkt aus einem Mail-Client ein Fax senden möchten, müssen Sie nur die Faxadresse im Mail-Format angeben: "faxnummer@fax.fax" oder "faxnummer@fax". Die Faxnummer muss immer in einem dieser zwei erlaubten Formate angegeben werden. Das Fax wird als ganz normale Mail erstellt. 602LAN SUITE erkennt eine solche Fax-Mail anhand des "fax"- oder "fax.fax"-Teils in der Adresse, wandelt sie in ein Fax um und sendet sie. Je nach Server-Konfigurationen können Sie auch Dokumente in verschiedenen Formaten (z.B. DOC, WPD, RTF, HTML, usw.) an die Mail anhängen. Sie können im Register "Fax" unter "OLE-Support" eine Liste der unterstützten Formate einsehen.

Faxnummer-Format beim Versand mittels Mail

Um Mails als Faxe zu versenden, ist es notwendig, die Faxnummer im Mail-Format anzugeben: "faxnummer@fax.fax" oder "faxnummer@fax". Die Faxnummer muss in einem der beiden erlaubten Formate angegeben werden: Vollständiges Format oder direktes Format.

Vollständiges Format - Das vollständige Format der Faxnummer enthält immer die Landeskennziffer, die Ortskennzahl (Ortsvorwahl) und die eigentliche Nummer mit Bindestrichen getrennt.

Die Nummer kann keine "0" zur Amtsholung, für Ferngespräche oder internationale Anrufe enthalten. Um das vollständige Format zu verwenden, ist es erforderlich, die die Wähleinstellungen und den Ort im Windows-Betriebssystem einzustellen (siehe Register "Fax" unter "Wähleinstellungen"). Dort müssen Sie alle Wähleigenschaften eingeben:

- Land
- Ortskennzahl
- Amtskennziffer für Ortsgespräche
- Amtskennziffer und Netzkennzahl für Ferngespräche

Die Telefonnummer, die Sie in der Mail-Adresse angegeben haben, wird mit den Wähleinstellungen verglichen.

- Wenn Sie als Land Amerika und als Ortskennzahl 904 eingestellt haben, jedoch eine Nummer wählen, die nicht zur Ortskennzahl passt (z.B. 305-56667777), wird die Nummer 13056667777 gewählt.
- Wenn Sie als Land Amerika und als Ortskennzahl 904 eingestellt haben und eine Nummer wählen, die zur eingestellten Ortskennzahl passt (z.B. 904-6667777), wird diese als lokale Nummer 6667777 gewählt.

Beispiel 1: 1-904-6667777@fax
Beispiel 2: 1-212-5559999@fax

Direktes Format - Die Nummer wird vor dem @ Symbol exakt so geschrieben, wie sie gewählt werden soll. Die Nummer darf keine Bindestriche, Klammern, Pluszeichen oder Leerzeichen als Formatierungssymbole enthalten! Geben Sie die Nummer exakt wie bei einem Telefon ein.

Beispiel 1: 6667777@fax
Beispiel 2: 13056667777@fax

Fax als Mail mit Anhang versenden

Die Mail, die Sie als Fax senden möchten, muss mitsamt der angehängten Dateien in ein grafisches Faxformat umgewandelt werden. Die Umwandlung kann direkt auf dem Client-Computer durch das 602LAN SUITE SendFax-Programm oder auf dem 602LAN SUITE-Server stattfinden. Der Server unterstützt eine große Anzahl von Formaten:

- **Interne Umwandlungsroutinen** – Zur Umwandlung von Text und Bitmap-Grafiken. Intern unterstützte Dateiformate: TXT, BMP, CLP, DCX, DIB, GIF, CUT, JPG, PCX, TIF, WMF.
- **Externe Routinen** – Für die Umwandlung bestimmter Dateiformate in das Faxformat durch Drucken im Hintergrund mit dem Fax602-Druckertreiber.

Welche Formate extern unterstützt werden, hängt davon ab, welche Programme auf dem Computer, auf dem 602LAN SUITE läuft, installiert sind:

- **DOC:** Word7 oder neuer, 602Text
- **XLS:** Excel97 oder neuer
- **WPD:** 602Text
- **RTF:** Word7 oder neuer
- **HTM, HTML:** MSIE 4 oder neuer, Word97 oder neuer

Die auf dem Server unterstützten externen Formate werden unter "Einstellungen/Erweiterte Konfiguration" im Register "Fax" unter "OLE-Support" aufgelistet.

HINWEIS: In einigen Anwendungen ist es erforderlich, den Fax602-Treiber als Standarddruckertreiber einzustellen.

Gemeinsamen Internet-Zugang konfigurieren (NAT)

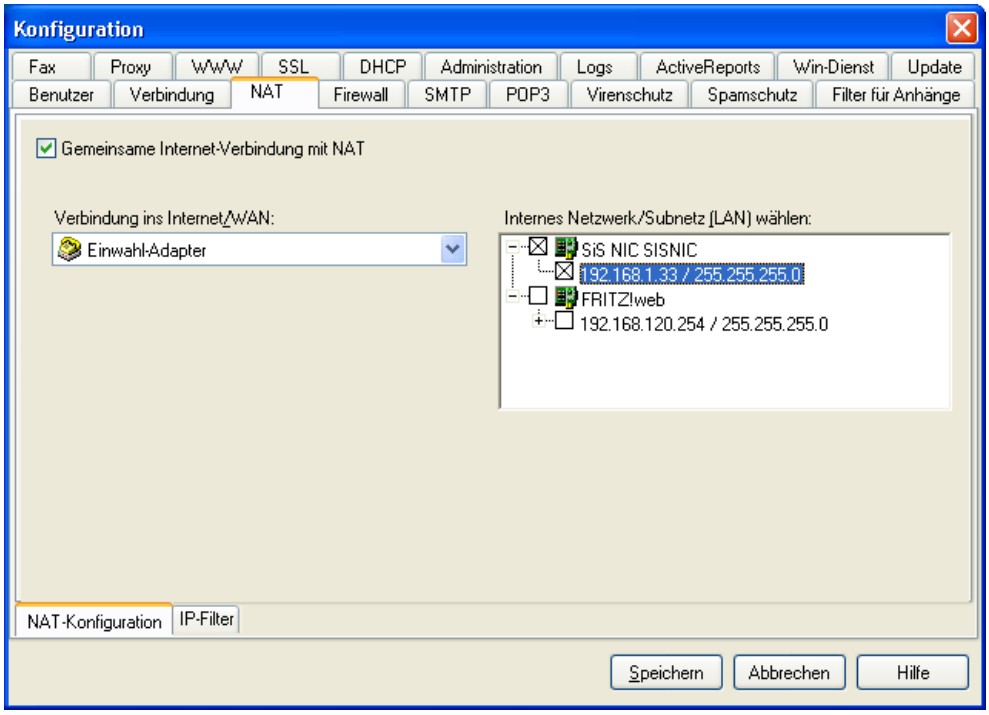
Für den gemeinsamen Internet-Zugang über 602LAN SUITE muss zuerst der Server so eingestellt werden, dass er NAT erlaubt. Danach müssen die TCP/IP-Gateways der Clients auf die IP-Adresse des 602LAN SUITE-Servers gesetzt werden. Letzteres geht automatisch, wenn Sie DHCP verwenden. Wenn Sie eine Benutzer-Authentifizierung oder eine Zugriffskontrolle verwenden wollen, müssen Sie den Internet-Zugang über den Proxy-Dienst einrichten (siehe nächstes Kapitel).

Was ist Network Address Translation (NAT)?

NAT (Network Address Translation) ist die Übersetzung einer IP-Adresse (Internet-Protokoll-Adresse), die in einem Netzwerk (Ihrem privaten Netzwerk) verwendet wird, zu einer anderen IP-Adresse, die in anderen Netzwerken (dem Internet) bekannt wird. NAT wandelt lokale Netzwerkadressen in eine oder mehr globale IP-Adressen und wandelt die globalen IP-Adressen von ankommenden Pakten wieder in die lokalen IP-Adressen. So wird eine gewisse Sicherheit geboten, da jede abgehende oder ankommende Anfrage durch einen Übersetzungsprozess läuft, der auch die Möglichkeit bietet die Anfrage zu qualifizieren, zu authentifizieren oder mit einer vorhergehenden Anfrage zu vergleichen. NAT behält außerdem die Anzahl der benötigten IP-Adressen und erlaubt es, mit einer einzigen IP-Adresse mit dem Internet zu kommunizieren.

NAT aktivieren

Um NAT in der 602LAN SUITE verwenden zu können, müssen Sie es in der Erweiterten Konfiguration aktivieren. Zudem muss die Verbindung ins Internet und das interne Netzwerk (LAN) ausgewählt werden.

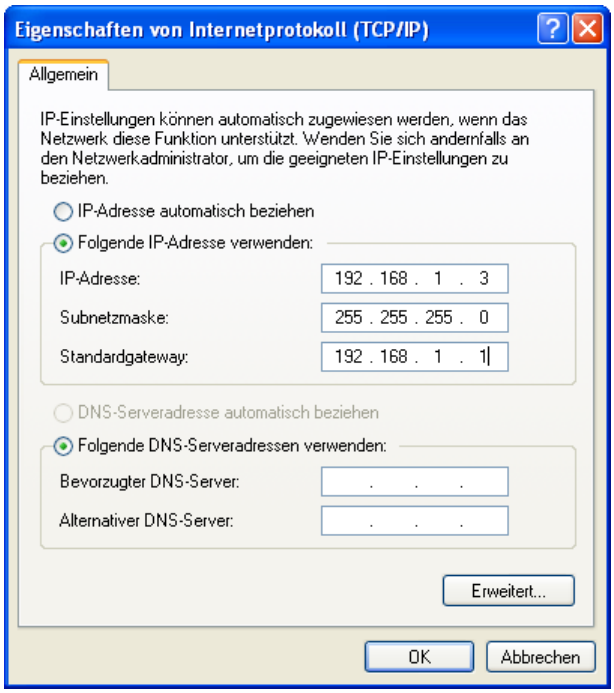


NAT-Konfiguration

Es ist notwendig, dass der Computer, auf dem 602LAN SUITE läuft, mindestens zwei Interfaces hat (z.B. zwei Netzwerkkarten oder eine Netzwerkkarte und einen Einwahl-Adapter). Wählen Sie zuerst die Verbindung ins Internet (WAN) und dann das interne Netzwerk (LAN) auf denen NAT arbeiten wird. Wenn ein Interface mehr als eine IP-Adresse hat, dann können Sie das gemäß Ihren Bedürfnissen einstellen.

LAN-Workstation-Einstellungen für NAT

Die Workstations im LAN müssen Ihre IP-Adressen im gleichen Netzwerk wie das interne Interface der 602LAN SUITE haben und dieses interne Interface muss in den Windows-Gateway-Einstellungen (Teil der Windows-TCP/IP-Einstellungen) eingetragen sein. Die TCP/IP-Einstellungen des Client-Computers werden bei Verwendung von DHCP automatisch eingestellt. Bei der manuellen Konfiguration müssen Sie die Gateway-IP-Adresse auf die des 602LAN SUITE-Servers einstellen. Öffnen Sie hierzu die Eigenschaften Ihrer Netzwerkverbindung (Systemsteuerung/Netzwerkverbindungen) und dort die Eigenschaften des TCP/IP-Protokolls.


Eigenschaften von Internetprotokoll (TCP/IP)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 1 . 3
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: 192 . 168 . 1 . 1
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server:
Alternativer DNS-Server:
Erweitert...
OK
Abbrechen

Beispiel:
Ein Computer, auf dem 602LAN SUITE läuft, hat ein internes Interface mit der IP-Adresse 192.168.1.1 und der Maske 255.255.255.0. Eine Workstation, die auf die 602LAN SUITE NAT zugreifen soll, muss daher wie folgt konfiguriert sein:

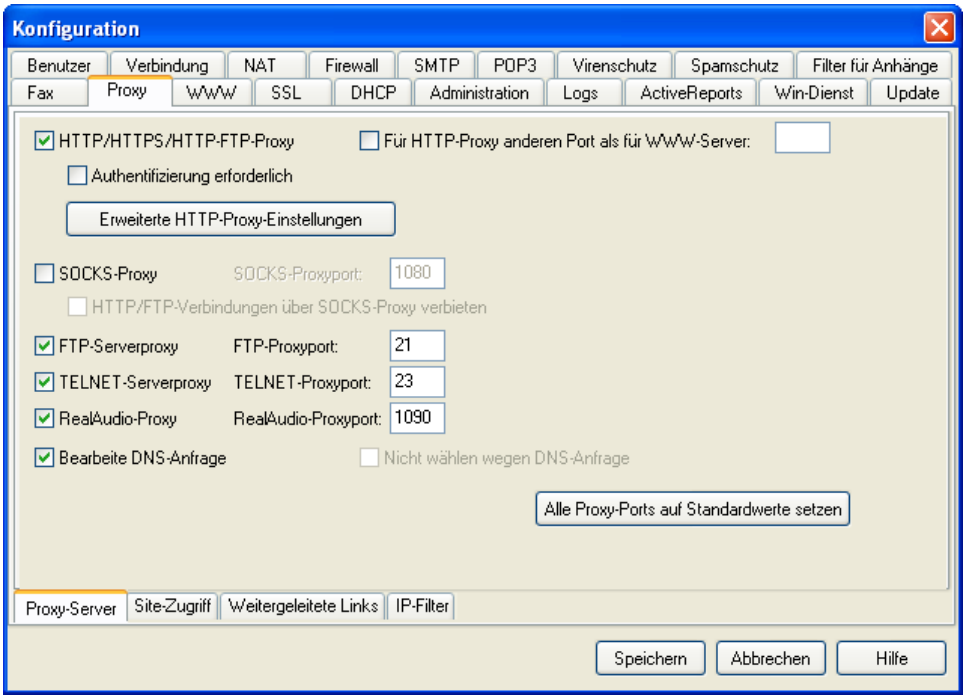
IP-Adresse: 192.168.1.x (x ist eine Zahl von 2 – 254)
Maske: 255.255.255.0
Gateway: 192.168.1.1

Hinweis:

- Es ist nicht möglich, ein LAN-Workstation vom Internet aus anzusprechen. NAT schützt das interne Netzwerk (Workstations) vor jedem Zugriff aus dem Internet.
- Network Address Translation (NAT) wird auf dem internen Interface ausgeführt. Daher ist der 602LAN SUITE-Computer komplett vom Internet aus zugänglich.
- Wenn interne (LAN) Workstations auf das interne Interface der 602LAN SUITE zugreifen, wird NAT **nicht** ausgeführt.
- Wenn interne (LAN) Workstation auf das externe Interface der 602LAN SUITE zugreifen, wird NAT ausgeführt.
- Wenn interne (LAN) Workstation auf andere Workstations im Netzwerk zugreifen, die auf dem externen Interface von 602LAN SUITE liegen, wird NAT ausgeführt.
- 602LAN SUITE bietet NAT für aktives FTP und Ping, nicht aber für Tracert
- 602LAN SUITE bietet kein NAT auf Computern mit mehreren Prozessoren oder Hyper-Threading.
- 602LAN SUITE bietet kein NAT für NetMeeting, IPsec, UpnP
- NAT öffnet keine Einwahl-Verbindung.

Gemeinsamen Internet-Zugang konfigurieren (Proxy)

Um einen gemeinsamem Internet-Zugang durch 602LAN SUITE zu konfigurieren, müssen Sie zunächst auf dem Server den Proxy und dann auf dem Client den Webbrowser konfigurieren. Wenn Sie für zusätzliche Netzwerk-Kontrolle die Benutzer-Authentifizierung einschalten möchten, müssen Sie, wie im Abschnitt zum Einrichten von Benutzern beschrieben, Benutzerkonten einrichten.



Die Proxies einrichten

Ein Proxyserver läuft auf einem Computer, der mit einer permanenten oder einer Einwahlverbindung mit dem Internet verbunden ist. Der Proxyserver empfängt Anforderungen der Client-Computer aus dem lokalen Netzwerk und leitet Sie in das Internet weiter. Antworten auf Anforderungen (z.B. HTML-Seiten) leitet er dann wieder an den entsprechenden lokalen Computer weiter. Der Proxyserver bietet zwei Funktionen:

- **Proxy** – Er arbeitet für Clients im lokalen Netzwerk als ein Proxy, der sie über die HTTP/HTTPS/HTTP-FTP Anwendungsprotokolle mit dem Internet verbindet.
- **Sicherheit** – Da alle Internet-Kommunikation über den Server läuft, kann dieser jede Verbindung über das HTTP/HTTPS/HTTP-FTP-Anwendungsprotokoll überprüfen.

Das Register "Proxy" finden Sie, wenn Sie "Einstellungen/Erweiterte Konfiguration" aus dem Menü von 602 Pro 602LAN SUITE 2004 auswählen. Standardeinstellung ist unbeschränkter Internet-Zugriff. Diese Einstellungen müssen in den meisten Fällen nicht geändert werden. Sie können Sie jedoch an Ihre individuellen Bedürfnisse oder Sicherheitserfordernisse anpassen. Sie können jeden 602LAN SUITE Proxydienst ein- oder ausschalten oder dessen Portnummer ändern. Alle Ports sind standardmäßig auf übliche Standards eingestellt. Sie können folgende Proxydienste an Ihre Bedürfnisse anpassen:

- **HTTP/HTTPS/HTTP-FTP** – Dies ist ein Proxy, der über verschiedene Varianten des HTTP-Protokolls Zugriff auf Internet-Webseiten bietet.
- **SOCKS** – Das SOCKS-Protokoll wird von vielen Instant Messaging-Programmen verwendet als auch von Programmen, die keine direkte Proxy-Unterstützung bieten. Die Standards SOCKS 4 und SOCKS 5 werden unterstützt.
- **FTP** – Dieser Proxy steuert das FTP-Protokoll (File Transfer Protocol), welches dazu verwendet wird, Dateien zu übertragen.
- **Telnet** – Dieser Proxydienst gestattet die Kommunikation von Telnet-Anwendungen über den 602LAN SUITE-Server.
- **RealAudio** – Dieser Proxy ist speziell dazu gedacht, die Benutzung des beliebten RealAudio-Programms von Real Networks, Inc. zu ermöglichen.

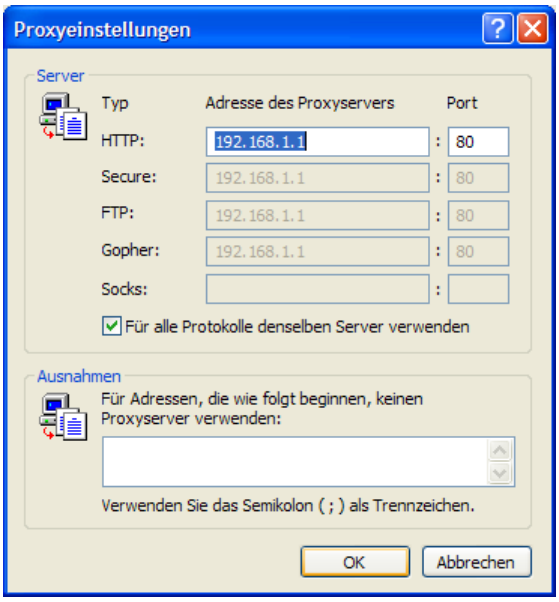
- **DNS-Anforderungen** – Dies ist kein echter Proxydienst. Der 602LAN SUITE-Server kann DNS-Anforderungen (Domain Name Server) für andere Computer im lokalen Netzwerk ausführen. Dies ist nützlich, wenn Sie ältere Anwendungen, die das SOCKS 4-Protokoll benutzen, verwenden möchten.

HINWEIS: Um alle Proxydienste auszuschalten, müssen Sie alle Auswahlfelder für Proxydienste deaktivieren.

Der HTTP/HTTPS/HTTP-FTP-Proxyserver läuft standardmäßig auf Port 80. Wenn Sie einen Webserver eines Drittanbieters verwenden, müssen Sie vielleicht einen anderen Port wählen, um Konflikte zu vermeiden. Es gibt keine Konflikte, wenn der Proxyserver zusammen mit dem im 602LAN SUITE 2004 eingebauten Webserver läuft.

Microsoft® Internet Explorer einrichten

Hier erfahren Sie, wie Sie den Microsoft Internet Explorer für die Verwendung mit dem Proxyserver einrichten können. Sie können die folgenden Anweisungen entsprechend auch als Hilfe zur Einrichtung anderer Webbrowser verwenden.
HINWEIS: Bitte beachten Sie, dass die automatische Proxyserver-Erkennung nicht unterstützt wird.



Microsoft® Internet Explorer Proxy-Einrichtung

1. Starten Sie Microsoft Internet Explorer
2. Wählen Sie "Extras/Internetoptionen" aus dem Menü.
3. Aktivieren Sie das Register "Verbindungen"
4. Klicken Sie im Bereich "LAN-Einstellungen" auf die Schaltfläche "Einstellungen".
5. Wählen Sie "Proxyserver für LAN verwenden" und klicken Sie dann auf "Erweitert...".
6. Geben Sie als Adresse des Proxyservers die IP-Adresse Ihres 602LAN SUITE-Servers an (z.B. 192.168.1.1)
7. Verwenden Sie für SOCKS den Port 1080. Für alle anderen Protokolle verwenden Sie die in der Abbildung gezeigten Ports.
8. Klicken Sie "OK", nochmal "OK" und dann noch ein letztes Mal "OK".

HINWEIS: Jede Anwendung mit Proxyserver-Unterstützung kann mit dem 602LAN SUITE-Proxyserver verwendet werden. Bitte lesen Sie in der Hilfedatei der Anwendung, um herauszufinden, wie Sie sie für Proxy-Unterstützung konfigurieren können.

Grundlegende Administration

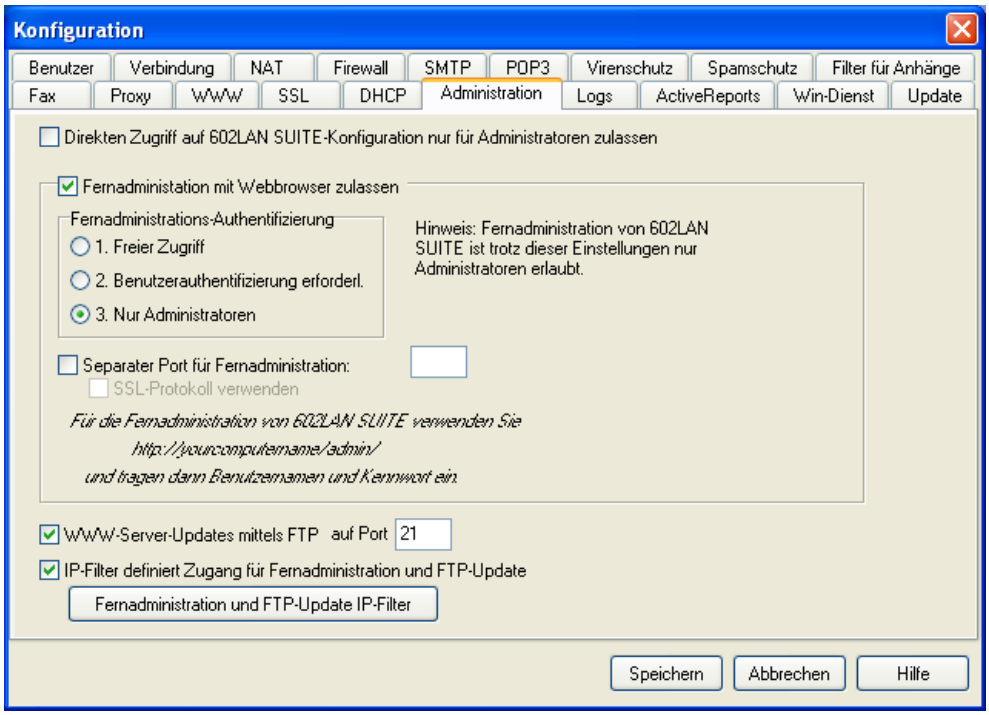
602LAN SUITE kann auf zwei verschiedene Arten administriert werden:

- Durch die Anwendung
- Über das webbasierte Administrationswerkzeug

Während beide Methoden ähnliche Möglichkeiten bieten, hat jede Methode Ihre Vorteile.

Administration konfigurieren

Administrationsoptionen werden im Register "Administration" konfiguriert. Sie können den direkten Zugriff auf die Programmkonfiguration nur Administratoren gestatten, sobald mindestens ein Benutzer Administrator-Rechte hat. Andernfalls ist das Auswahlfeld "Direktzugang zur 602LAN SUITE-Konfiguration nur für Administratoren zulassen" schattiert und nicht verfügbar.



Aktualisieren des WWW-Servers mittels FTP

HTML-Seiten werden auf dem 602LAN SUITE-WWW-Server in dem Ordner gespeichert, der im WWW-Register festgelegt wurde. standardmäßig ist das /DOCS. Sie können die Seiten direkt verwalten oder per Fernzugriff (Remote) mittels HTTP- oder FTP-Protokoll. Um das Aktualisieren mittels FTP zu erlauben, müssen Sie die Option „WWW-Server-Updates mittels FTP auf Port xyz“ aktivieren. Der Standardport für FTP ist 21.

HINWEIS: Um einen anderen FTP-Server als den der 602LAN SUITE einzusetzen, sollten Sie einen anderen Port verwenden (z.B. 8021 – dann können Sie immer noch auf den 602LAN SUITE FTP-Server zugreifen, ohne mit der anderen FTP-Software in Konflikt zu geraten).

Fernadministration- und FTP-Update-IP-Filter

Der Fernadminstrations- und FTP-Update-IP-Filter legt fest, welche Verbindungen Zugriff auf die Webadministration und den FTP-Update-Server erhalten. Die IP-Filterregeln werden **von oben nach unten** durchgearbeitet, wobei die unteren Regeln die oberen überstimmen können. Geben Sie die IP-Adresse und Maske des Computers oder Netzwerks an, das die Anfrage senden soll. Dabei ist es notwendig bei jedem Eintrag festzulegen, ob er erlaubt oder verweigert wird – ROT bedeutet „Zugriff verweigern“, GRÜN bedeutet „Zugriff erlauben“.

Administration durch die Anwendung

Diese Optionen bieten Ihnen vollständigen, unbeschränkten Zugang zu allen Administrationsoptionen von 602LAN SUITE. Sie können 602LAN SUITE als Windows-Dienst einrichten und die Optionen, die die Administration steuern, ändern. Der Nachteil ist, dass Sie direkt am Server sitzen oder von einem entfernten Computer auf die grafische Oberfläche des Server-Computers zugreifen müssen (Remote Access).

Webbasierte Administration

Die webbasierte Administration gibt dem Administrator die Möglichkeit, von jedem Computer im lokalen Netzwerk und bei entsprechender Konfiguration auch von jedem Computer im Internet Einstellungen zu ändern, Benutzerkonten zu konfigurieren und Dienste-Parameter anzupassen. Nachteil dieser Annehmlichkeit ist, dass die Optionen zur Steuerung der Administration und zur Einrichtung von 602LAN SUITE als Windows-Dienst nicht zugänglich sind. Dies ist im Allgemeinen kein Problem, da diese Möglichkeiten bei der täglichen Administration keine große Rolle spielen. Sie werden einmal eingerichtet und dann in der Regel nicht mehr geändert.

HINWEIS: Wenn Sie 602LAN SUITE als Windows-Dienst laufen lassen, müssen Sie entweder die webbasierte Administration verwenden oder den Dienst stoppen, bevor Sie die 602LAN SUITE-Anwendung starten.

Auf das webbasierte Administrationswerkzeug zugreifen

Um die Fernadministration aufzurufen, starten Sie auf einem mit dem lokalen Netzwerk verbundenen Computer einen Webbrowser und geben Sie die folgende Adresse ein, bei der Sie "ihrserver" durch den Namen oder die IP-Adresse Ihres 602LAN SUITE-Servers ersetzen:

http://ihrserver/admin

Sobald Sie eine Verbindung mit dem 602LAN SUITE WWW-Server aufbauen, werden Sie aufgefordert, sich mit Benutzernamen und Kennwort anzumelden. Sie können den Zugriff auf die Fernadministration im Register "Administration" auf Administratoren beschränken. Andernfalls hat jeder gültige 602LAN SUITE-Benutzer Zugang auf die Fernadministration.

HINWEIS: Wenn Sie IP-Filterregeln verwenden möchten, um die Fernadministration zu sichern und Computern mit IP-Adressen außerhalb Ihres lokalen Netzwerkes oder unautorisierte IP-Adressen den Zugang zu verweigern, wählen Sie im Register "Administration" die Option "IP-Filter definiert Zugang für Fernadministration und FTP-Update".

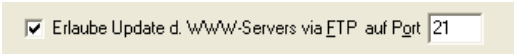
WWW-Server und webbasierte Administration

Die Fernadministration läuft über den eingebauten WWW-Server von 602LAN SUITE und folgt daher den Regeln, die Sie im Register "WWW" definieren. Wenn Sie Ihren WWW-Server nur auf einer Netzwerk-Schnittstelle zu Ihrem lokalen Netzwerk laufen lassen, können auch nur Computer aus Ihrem lokalen Netzwerk auf die Fernadministration zugreifen. Wenn Sie den WWW-Server auf allen Schnittstellen laufen lassen, kann ein Administrator den 602LAN SUITE-Server von jedem Computer, der mit dem Internet verbunden ist, administrieren. Zusätzlich dazu beachtet die Fernadministration auch die in Register "WWW" definierten Regeln für den IP-Filter.

Den WWW-Server von einem entfernten Computer mittels FTP aktualisieren

HTML-Seiten auf dem 602LAN SUITE WWW-Server sind im Startverzeichnis für den WWW-Server untergebracht (siehe das Register "WWW"). Das Standardverzeichnis ist "/DOCS" innerhalb des 602LAN

SUITE-Programmordners. Sie können die Dateien in diesem Verzeichnis direkt von dem Computer aus verwalten, auf dem 602LAN SUITE läuft, oder von einem anderen Computer über das HTTP- oder FTP-Protokoll. Um die Aktualisierung von WWW-Seiten mittels FTP zu erlauben, aktivieren Sie im Register "WWW" die Option "Erlaube Updates des WWW-Servers mittels FTP". Der Standard-Port für FTP ist 21.



HINWEIS: Um einen anderen FTP-Server als den von 602LAN SUITE zu verwenden, benutzen Sie einen anderen Port (z.B. 8021). So können Sie auf den FTP-Dienst von 602LAN SUITE zugreifen, ohne die andere FTP-Server-Software zu stören.

Es gibt verschiedene Wege, um HTML-Seiten auf dem Server zu verwalten.

Sie können HTML-Seiten mit jedem FTP-Client an den 602LAN SUITE FTP-Server senden:

- Wenn Sie den Netscape Navigator verwenden, benutzen Sie den eingebauten HTML-Editor (Netscape Composer) und das Publizieren-Symbol - Protokoll: HTTP PUT.
- Wenn Sie Microsoft Internet Explorer verwenden, nutzen Sie den Web Publishing Assistenten (standardmäßig in Windows 98, MSIE 4.0 oder neuer und FrontPage) – HTML-Seiten werden über das FTP-Protokoll übertragen.

Wer den WWW-Server verwalten darf

Nur 602LAN SUITE-Administratoren dürfen den 602LAN SUITE WWW-Server verwalten. Ein regulärer Benutzer darf nur seine eigene persönliche Webseite verwalten.

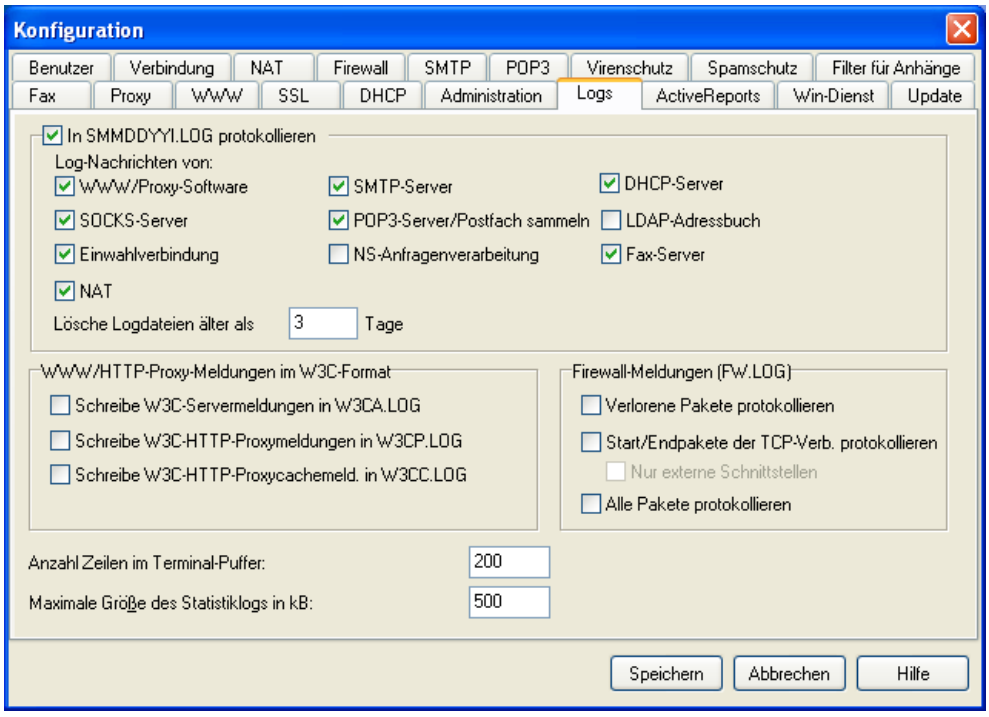
IP-Filter für Fernadministration und FTP-Update

Dieser IP-Filter definiert anhand von Regeln den Zugang zur Fernadministration und zum FTP-Update. Die IP-Filter-Regeln werden von oben nach unten überprüft. Jede nachfolgende Regel überstimmt gegebenenfalls die vorhergehenden Regeln. Geben Sie die IP-Adresse und die Maske des Computers oder Netzwerks an, das die Anforderung sendet, in die Felder "IP-Adresse" und "IP-Maske" ein. Definieren Sie dann, ob dem betreffenden Computer oder Netzwerk der Zugang erlaubt oder verweigert wird! ROT bedeutet Zugang verweigern, GRÜN bedeutet Zugang erlauben.

Server-Aktivität protokollieren

Protokolle (Logs)
602LAN SUITE listet im Hauptfenster alle Serveraktivität auf. Dieses Protokoll kann auch in eine Datei gespeichert werden. 602LAN SUITE bietet das Protokollieren von WWW- und HTTP-Proxyserver-Aktivitäten im W3C-Format für die spätere Analyse durch Programme wie z.B. die 602LAN SUITE-Erweiterung ActiveReports oder das Analysetool Sawmill (siehe http://sawmill.haage-partner.de).

- **Anzahl Zeilen im Terminal-Puffer:** Geben Sie die Anzahl der Zeilen an, die maximal im Hauptfenster angezeigt werden können. Beim Überschreiten der Anzahl werden die ältesten Einträge gelöscht.
- **In SMMDDYY.LOG protokollieren:** Protokolliert die Serveraktivitäten in eine Datei. Dabei wird für jeden Tag eine Protokolldatei angelegt. Diese Dateien befinden sich im 602LAN SUITE-Programmverzeichnis. Der Dateiname folgt dem Schema SMMDDYYI.LOG (MM für den Monat, DD für den Tag und YY für das Jahr). Jede Datei wird so viele Tage lang aufgehoben, wie Sie unter "Lösche Logdateien älter als x Tage" angeben und danach gelöscht.
- **Maximale Größe des Statistiklogs in KB:** Es gibt ein weiteres Protokoll: lansuite.csv. Diese Datei wird automatisch erstellt, sobald das erste Fax versendet wird, und protokolliert nur den Faxversand. Die Maximalgröße dieser Datei wird durch diese Option begrenzt. Sobald die angegebene Größe erreicht wird, wird die Datei um 10% gekürzt und dann weiter protokolliert.



Unter "Log-Nachrichten von" können Sie einstellen, welche Dienste protokolliert werden sollen:
- WWW/Proxy-Software
- SOCKS-Server
- Einwahlverbindung
- NS-Anfragenverarbeitung
- DHCP-Server
- SMTP-Server
- POP3-Server/Postfach sammeln
- LDAP-Adressbuch
- Faxserver
- NAT

W3C – Erweitertes Protokolldatei-Format
Die meisten Webserver bieten die Option, Protokolle im allgemeinen Protokoll-Format (Common Log Format) (http://www.w3.org/Daemon/User/Config/Logging.html#common-logfile-format) oder einem proprietären

Format zu speichern. 602LAN SUITE unterstützt die folgenden Protokolldateien im erweiterten Protokolldatei-Format des W3C (Extented Log File Format):

- **W3CA.LOG** - WWW-Server-Protokolldatei
- **W3CP.LOG** - Proxyserver-Protokolldatei
- **W3CC.LOG** - Cache Proxyserver-Protokolldatei

W3C-Protokolldateien werden in einem Format gespeichert, das von Analyse-Werkzeugen wie Sawmill (siehe http://sawmill.haage-partner.de) ausgewertet werden kann. Im Dateikopf einer Protokolldatei wird deren Datentyp angegeben.

Firewall-Nachrichten

Firewall-Nachrichten werden in die Datei "FW.LOG" protokolliert. Die Optionen definieren, welche Informationen protokolliert werden:

- Verlorene Pakete protokollieren – Verlorene Pakete werden protokolliert
- Start-/Endpakete der TCP-Verb. protokollieren – Protokolliert den Anfang und das Ende jeder TCP-Verbindung.
- Alles Pakete protokollieren – Der komplette Datenaustausch wird protokolliert (**WARNUNG**: Sollte nur zur Fehlersuche verwendet werden, da die Logdatei sehr schnell sehr groß wird!).

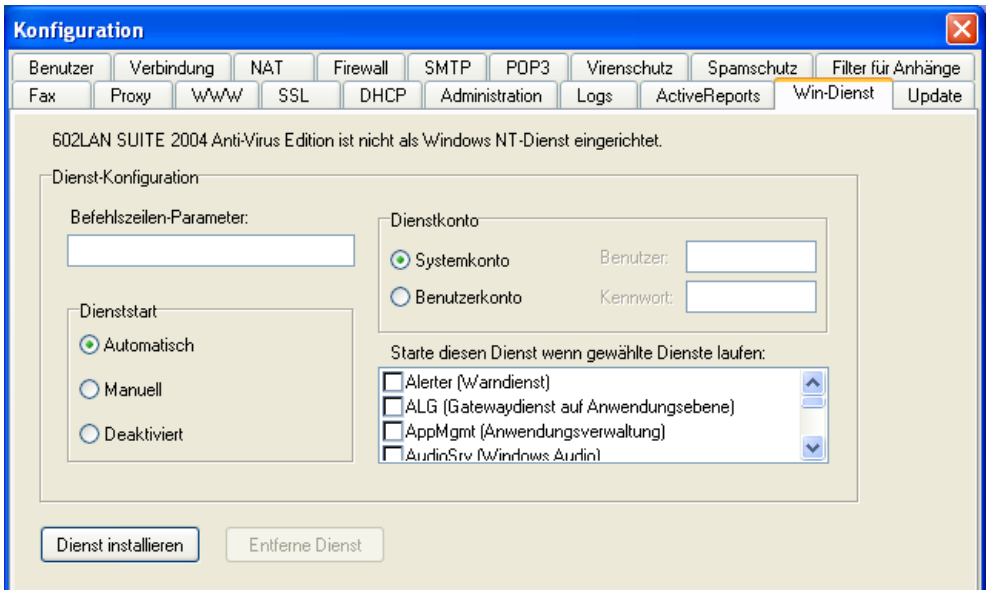
Als Windows-Dienst installieren

Win-Dienst

Das Register „Win-Dienst" wird angezeigt, wenn 602LAN SUITE unter Windows NT/2000/XP/2003 läuft. Die erste Zeile zeigt, ob 602LAN SUITE gegenwärtig als Windows-Dienst läuft. Hier können Sie den 602LAN SUITE-Server als Windows-Dienst einrichten und konfigurieren:

- **Befehlszeilen-Parameter** – Hier geben Sie die Parameter an, mit denen der Dienst gestartet wird.
- **Dienststart** – Hier geben Sie an, ob der Dienst automatisch beim Systemstart gestartet werden soll, ob der Benutzer ihn manuell aus der Systemsteuerung (Dienste) starten muss oder ob der Dienst abgeschaltet sein soll.
- **Dienstkonto** – Hier weisen Sie dem Dienst ein Konto zu, das die Rechte des Dienstes definiert. Wenn 602LAN SUITE zum Beispiel das Recht benötigt, auf Netzwerk-Laufwerke zuzugreifen, müssen Sie das Konto eines Benutzer angeben, der das Recht hat, auf diese Laufwerke zuzugreifen.
- **Starte diesen Dienst, wenn gewählte Dienste laufen** – Manchmal ist es erforderlich sicher zu stellen, dass bestimmte Dienste geladen werden, bevor der 602LAN SUITE-Dienst gestartet wird. Hier können Sie diese Dienste angeben, damit 602LAN SUITE erst startet, wenn diese Dienste bereits laufen.

Klicken Sie die Schaltfläche "Dienst installieren", um 602LAN SUITE als Dienst zu installieren. Verwenden Sie die Schaltfläche "Dienst entfernen", um den Dienst wieder zu entfernen.



HINWEIS: Dies hat keinen Effekt auf den aktuellen Zustand des Dienstes (wenn 602LAN SUITE gerade als Dienst läuft, müssen Sie diesen Dienst manuell beenden).

Win98-Dienst

Wenn Sie Win98 verwenden, erscheint das Register "Win98-Dienst". Hier können Sie 602LAN SUITE als Windows 98-Dienst einrichten. Die erste Zeile zeigt, ob 602LAN SUITE gegenwärtig als Windows 98-Dienst installiert ist. Mit Windows 98-Dienst ist gemeint, dass Sie 602LAN SUITE automatisch beim Systemstart starten lassen können. Das Symbol von 602LAN SUITE finden Sie dann im unteren rechten Bereich der Windows-Taskleiste. Geben Sie bei Bedarf Befehlszeilen-Parameter in das entsprechende Feld ein. Um 602LAN SUITE als Windows 98-Dienst zu installieren, klicken Sie "Dienst installieren". Um den Dienst zu entfernen, klicken Sie "Dienst entfernen".

HINWEIS: Wenn Sie 602LAN SUITE als Windows-Dienst laufen lassen, müssen Sie entweder die webbasierte Administration verwenden oder den Dienst stoppen, bevor Sie die 602LAN SUITE-Anwendung starten.

DHCP-Server einrichten

Das DHCP-Protokoll (Dynamic Host Configuration Protocol) dient dem Austausch grundlegender TCP/IP-Einstellungen. Ein Computer im lokalen Netzwerk kann beim DHCP-Server eine IP-Adresse anfordern sowie Netzwerk-Maske, DNS-Server und andere Einstellungen erfragen. Die dynamische Zuteilung von IP-Adressen erleichtert die Administration und bietet eine effiziente Verwaltung der verfügbaren IP-Adressen: Nur Computer, die gerade in Betrieb sind, erhalten IP-Adressen. DHCP verwendet das UDP-Protokoll auf Port 67 und 68. DHCP ist ein offener Standard, der von der Dynamic Host Configuration Working Group (DHC WG) der Internet Engineering Task Force (IETF) entwickelt wird. Das DHCP-Protokoll ist von den Protokollen RARP, DRARP und BOOTP abgeleitet. Eine vollständige Beschreibung findet man in RFC 2131, 1531, 1541, 1534 und 2132.

Den DHCP-Server einschalten

Um den DHCP-Server von 602LAN SUITE zu verwenden, müssen Sie ihn zuerst aktivieren. Stellen Sie dann sicher, dass für den DHCP-Server die IP-Adresse IHRES LOKALEN Netzwerks ausgewählt ist.

IP-Bereiche einrichten

Definieren Sie eine "Start-IP-Adresse" und eine "End-IP-Adresse", die den Bereich der IP-Adressen angibt, der vom DHCP-Server für anfragende Computer verwendet werden kann. Klicken Sie auf "Hinzu", wenn Sie sie eingegeben haben. Um einen IP-Bereich zu löschen, wählen Sie ihn aus und klicken Sie auf "Löschen". Es können mehrere IP-Bereiche definiert werden.

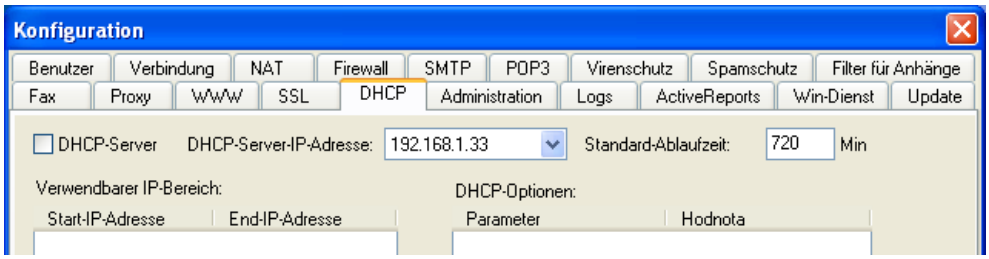
Empfehlung: Wir empfehlen Klasse C IP-Adressen wie 192.168.x.x zu verwenden. Die Start-IP-Adresse sollte 192.168.1.10 lauten. Die End-IP-Adresse kann bis hin zu 192.168.1.254 gehen. Wenn Sie mit 192.168.1.10 starten, geben Sie sich selbst 9 IP-Adressen, die Sie für Server und Computer verwenden können, die DHCP nicht nutzen sollen. Diese IP-Adressen sind 192.168.1.1 bis 192.168.1.9.

DHCP-Optionen

Es gibt viele DHCP-Optionen und -Variablen, die 602LAN SUITE unterstützt, doch Sie brauchen nur 2 davon:

- **Subnetz-Maske:** Diese Option sollte auf 255.255.255.0 gesetzt sein.
- **Domain Name Server:** Diese Option sollte auf die IP-Adresse Ihres Proxyservers gesetzt sein (die IP-Adresse des Computers auf dem 602LAN SUITE läuft).

Wählen Sie die gewünschte DHCP-Option, geben Sie dann den "DHCP-Optionswert" ein und klicken Sie dann auf "Hinzu". Um eine Option zu löschen, wählen Sie sie aus und klicken Sie auf "Löschen". Weitere Informationen zu DHCP und seine Optionen finden Sie auf http://www.dhcp.org.



Erweiterte Features

SMTP-Authentifikation & -Einstellungen

Erweiterte Sendeparameter

Einige Internetanbieter verlangen eine Authentifizierung, um Mails über ihren SMTP-Server zu versenden. Wenn Ihr Internetanbieter dies erfordert, aktivieren Sie "SMTP-Server erfordert Authentifizierung". Wählen Sie die Authentifizierungsmethode - "mittels SMTP" oder "mittels POP3" - und tragen Sie Benutzername und Kennwort ein. Die verwendete Authentifizierungsmethode erfahren Sie von Ihrem Internetanbieter.

Private Netzwerke

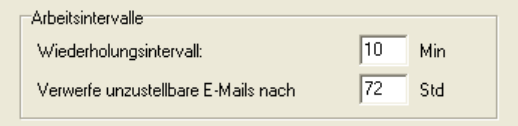
Sie können Mails anhand festgelegter Routen weiterleiten lassen, wenn Sie Mails statt an das Internet an bestimmte Computer weiterleiten möchten. Sie können festgelegte Routen definieren, wenn Sie die Option "Verwende festgelegte Routen" aktivieren. Sobald Sie die Schaltfläche "Festgelegte Routen" anklicken, erscheint eine Liste mit den festgelegten Routen. Geben Sie die "Maildomäne" und den "Ziel-Host" ein und klicken Sie auf "Neu". Sie können einen Eintrag löschen oder ändern, indem Sie die Schaltfläche "Löschen/Bearbeiten" anklicken. Klicken Sie wieder auf "Neu", wenn Sie einen Eintrag geändert haben.

DNS-Einstellungen

Geben Sie die IP-Adresse Ihres DNS-Servers ein (dieser wird Ihnen vom Internetanbieter zugewiesen). Sie können in die Felder "DNS1" und "DNS2" bis zu zwei DNS-Server eintragen. Wenn diese Felder leer sind, verwendet 602LAN SUITE die Einstellungen der TCP/IP-Konfiguration in Windows (siehe "Mails direkt mittels DNS an das Internet senden").

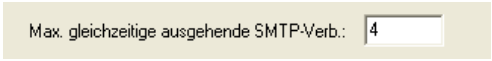
Arbeitsintervalle

Dieser Bereich dient dazu SMTP-Zeitintervalle zu setzen. Wenn eine Mail nicht gesendet werden kann (z.B. weil der entfernte SMTP-Server offline ist), wird nach einer bestimmten Zeit ein erneuter Versuch gestartet. Zusätzlich können Sie im Feld "Verwerfe unzustellbare Mails nach" die Zeit in Stunden angeben, nach der unzustellbare Mails verworfen werden sollen.



Maximale Anzahl gleichzeitig ausgehender SMTP-Verbindungen

Dies bestimmt die maximale Anzahl der gleichzeitig ausgehenden SMTP-Verbindungen. Wenn Sie über 602LAN SUITE eine große Anzahl von Mails versenden, können Sie die Sendegeschwindigkeit erhöhen, indem Sie diese Anzahl anheben. Dazu muss natürlich genügend Bandbreite vorhanden sein.

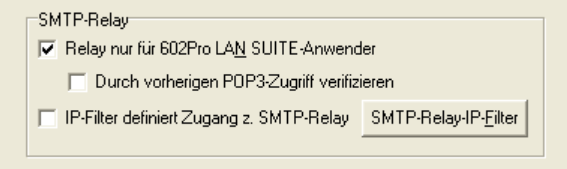


HELO/EHLO-Kommando

Hier können Sie einen vollständigen Domainnamen angeben, der zu Remote-SMTP-Servern geschickt wird.

SMTP-Relay-Optionen

Die SMTP-Relay-Funktion erlaubt die Weiterleitung von Mails, deren Empfänger (Adresse im "An:"-Feld) keine Benutzer mit Postfach auf dem 602LAN SUITE-Server sind. Diese Funktion ist für 602LAN SUITE-Benutzer erforderlich, damit diese mit Ihrem Mail-Programm über SMTP Mails an den 602LAN SUITE-Server senden können, die dieser dann ins Internet weiterleitet. Standardmäßig funktioniert diese Weiterleitung nur für 602LAN SUITE-Benutzer (Option "Relay nur für 602LAN SUITE-Benutzer"). Der SMTP-Server prüft die Mail-Adresse des Absenders (im "Vom:"-Feld) und verweigert die Weiterleitung, wenn die Mail-Adresse nicht mit einer Benutzer-Mail-Adresse oder einem Alias übereinstimmt. Wenn Sie die Option "Durch vorherigen POP3-Zugriff verifizieren" wählen, funktioniert die Weiterleitung nur, wenn der Benutzer vor dem SMTP-Zugriff mittels POP3 mit Benutzernamen und Kennwort auf sein Postfach zugegriffen hat. Wenn Sie möchten, dass JEDER Internet-Benutzer Mails versenden kann, deaktivieren Sie beide Optionen.



WARNUNG: Der SMTP-Server von 602LAN SUITE ist anfällig für Spam-Mißbrauch, wenn Sie beide Optionen deaktivieren! Wenn Sie den SMTP-Relay-Zugriff über den IP-Filter sichern möchten, aktivieren Sie die Option "IP-Filter definiert Zugang zum SMTP-Relay" und richten Sie den SMTP-Relay-IP-Filter ein.

SMTP-Relay-IP-Filter

Dieser IP-Filter definiert anhand von Regeln, welche Verbindungen über den SMTP-Server Mails weitergeben dürfen (SMTP-Relay). Die IP-Filter-Regeln werden von oben nach unten überprüft. Jede nachfolgende Regel überstimmt gegebenenfalls die vorhergehenden Regeln. Geben Sie die IP-Adresse und die Maske des Computers oder Netzwerks an, das die Anforderung sendet, in die Felder "IP-Adresse" und "IP-Maske" ein. Definieren Sie dann, ob dem betreffenden Computer oder Netzwerk der Zugang erlaubt oder verweigert wird! ROT bedeutet Zugang verweigern, GRÜN bedeutet Zugang erlauben.

Webmail

Der Webmail-Client macht die 602LAN SUITE-Postfächer über einen Webbrowser oder drahtlose Geräte, die das WAP-Protokoll (Wireless Access Protocol) unterstützen, zugänglich. Jegliche Kommunikation zwischen Browser (Client) und 602LAN SUITE (Server) läuft über das HTTP- oder das HTTPS-Protokoll (Secure HTTP).

Anmeldung beim Webmail-Client

Starten Sie einen Webbrowser und geben Sie die IP-Adresse oder den Namen des Computers an, auf dem 602LAN SUITE läuft (z.B. http://192.168.1.1/mail oder http://www.ihre-firma.de/mail):

1. Geben Sie Ihren Benutzernamen an. Beim Benutzernamen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
2. Geben Sie Ihr Kennwort ein. Beim Kennwort wird nicht zwischen Groß- und Kleinschreibung unterschieden.
3. Klicken Sie auf "Anmelden".

602 LAN SUITE
E-mail • Fax • Web
Anti-spam • Anti-virus
Proxy • Firewall/NAT
Bitte melden Sie sich an:
Benutzername:
Kennwort:
Anmelden
Benutzername und Kennwort merken
Wichtig! Denken Sie daran, sich abzumelden.
Denken Sie zu Ihrer Sicherheit immer daran, auf "Abmelden" zu klicken, wenn Sie fertig sind.
© Software602, Inc

HINWEIS: Wenn Sie länger als 60 Minuten inaktiv sind, meldet Sie der Webmail-Client automatisch ab.

Fenster des Webmail-Clients

Das Fenster des Webmail-Clients enthält zwei horizontale Bereiche - die Menüleiste und den Bereich, der der entsprechenden Funktion entspricht. Sie können die folgenden Funktionen nutzen:

- Neue Mail
- Postfach
- Adressbuch
- Optionen
- Hilfe
- Abmelden

"Hilfe" zeigt die Hilfeseite.
"Abmelden" meldet Sie vom Server ab.

Postfach

Jedes Benutzerpostfach hat die folgenden sechs Ordner: **Posteingang, Entwürfe, Postausgang, Gesendete Mails, Versandliste** und **Gelöschte Mails**.
Der linke Teil des Fensters zeigt den Ordnerbaum, rechts sind die Einträge im gewählten Ordner. Der erste Ordner im Ordnerbaum ist der **Posteingang**.

Eingang

Diese Funktion zeigt die empfangenen Mails. Auf der linken Seite des Fensters sehen Sie eine hierarchische Anzeige der Mail-Ordner. Der Anfang dieser Anzeige ist der Ordner "Posteingang". Sie können einen neuen Ordner erstellen, indem Sie den Namen des neuen Ordners in das Feld "Neuen Ordner erstellen" eingeben und dann die Eingabetaste drücken oder mittels Maus bestätigen, indem Sie den Haken anklicken. Für jede Mail gibt es ein Auswahlfeld, das Ihnen erlaubt, die Mails zu wählen, mit denen Sie arbeiten möchten (löschen, in eine andere Schublade kopieren oder verschieben). Das erste Auswahlfeld über allen anderen Auswahlfeldern wählt alle Mails aus.

Eine Mail hat drei Merkmale:

- Datum und Zeit
- Absender
- Betreff

Es ist möglich, Mails nach einem dieser Merkmale zu sortieren. Klicken Sie dazu einfach den entsprechenden Eintrag in der Titelzeile an.

Um eine Mail zu öffnen, klicken Sie auf den Link zu der Mail. Dieser befindet sich in der Zeile des Merkmals, nachdem sortiert wird. Die Schaltfläche direkt neben dem Titel des Mail-Ordners aktualisiert die Mail-Liste. Die Liste der Mails wird von 602LAN SUITE gelesen. Die Liste wird nicht automatisch aktualisiert.

Wenn Sie viele Mails in einem Ordner haben, können Sie mit den Pfeilsymbolen am Ende der Liste (<< und >>) blättern. In der Mitte zwischen den Pfeilsymbolen wird die aktuelle Position angezeigt.

Entwürfe

Der Ordner enthält die Mails, die Sie noch nicht fertig gestellt haben. Sie können Sie jederzeit weiter bearbeiten und versenden.

Postausgang

Dieser Ordner enthält die Mails, die darauf warten, versendet zu werden. Es ist möglich eine solche Mail zu überprüfen. Wählen Sie die zu prüfende Nachricht aus und klicken Sie den Deaktivieren-Schalter. Dann klicken Sie auf den Nachrichten-Link (je nachdem nach welchem Attribut sie sortiert wurde). Wenn Sie fertig sind, drücken Sie den Schließen-Schalter. Wenn Sie zufrieden sind, schalten Sie die Senden-Option wieder ein. Wenn Sie nicht zufrieden sind, können Sie die Mail auch löschen.

Gesendete Mails

Jede gesendete Mail wird in dieses Verzeichnis kopiert. Standardmäßig ist diese Funktion nicht aktiviert. Um Sie zu aktivieren, müssen Sie die Option „Kopie jeder verschickten Mail im Versendete Mails-Ordner speichern" im Optionen-Menü anhaken.

Versandliste

Dieser Ordner enthält eine Liste der gesendeten Mails. Der Inhalt der Mails kann jedoch nicht angesehen werden.

Gelöschte Mails

Wenn Sie eine Mail aus einem Verzeichnis löschen, wird sie zuerst hierher verschoben (unter Optionen können Sie auch einen anderen Ordner wählen).
Um eine Mail vollständig zu löschen, müssen Sie sie in diesem Ordner löschen. Um eine Mail wieder herzustellen, klicken Sie auf „Wiederherstellen".
Sie können den Inhalt dieses Ordners automatisch in regelmäßigen Intervallen löschen. Geben Sie dazu einen Wert bei „Mails nach x Tagen löschen“ und bestätigen Sie mit „OK“.
Um das Zeitintervall zu ändern, müssen Sie zuerst die Funktion deaktivieren und dann einen neuen Wert eingeben.

Eine neue Mail erstellen

Die Eingabemaske zum Erstellen einer neuen Mail enthält folgende Felder:

- **Von:** – Wenn Sie keine Aliase haben, wird nur eine Adresse angezeigt. Andernfalls können Sie einen Ihrer Aliase wählen.
- **An:** – Klicken Sie auf diesen Link, um Empfänger zu wählen. Das Adressbuch wird geöffnet. Oder tippen Sie die Adresse des Empfängers direkt ein.
- **Kopie (CC:)** – Klicken Sie auf diesen Link, um Empfänger zu wählen. Das Adressbuch wird geöffnet.
- **Anhänge:** – Es öffnet sich ein Fenster, um Dateien anzuhängen.
- **Betreff:** – Feld, um den Betreff einer Mail einzugeben. Dieser wird in der Mail-Liste des Empfängers angezeigt.
- **Mail-Textfeld** – Textfeld, um die eigentliche Nachricht zu schreiben.
- **Signatur** – Aktivieren Sie diese Option, wenn Sie möchten, dass die unter "Optionen" definierte Signatur an den Mail-Text angehängt werden soll.
- **Verdeckte Kopien (Blind Carbon Copy)** – Wenn Sie in den Feldern "Von:" oder "Kopie:" mehr als einen Empfänger angeben, und diese Option aktivieren, wird der Nachrichtenkopf die Adressen der jeweils anderen Empfänger nicht enthalten. Kein Empfänger erfährt von den anderen Empfängern.
- **Empfangsbestätigung anfordern** – Die Mail wird mit einer Bestätigungsanforderung verschickt. Der Empfänger wird gefragt, das Öffnen der Mail zu bestätigen, und Sie erhalten dann eine Bestätigung, dass der Empfänger Ihre Mail geöffnet hat. 602LAN SUITE erstellt eine solche Bestätigungs-Mail automatisch.
- **Format** – Format der Mail. Wählen Sie ein Standardformat: MIME, RFC822 oder UUEncode.

Rechtschreibprüfung

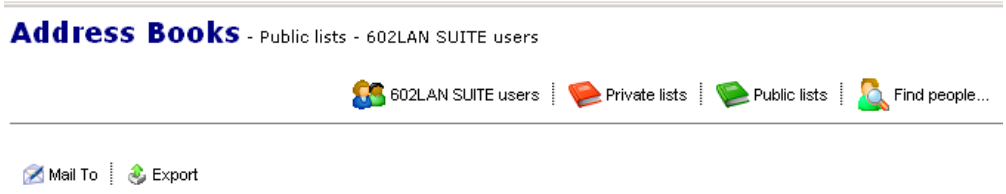
Die Rechtschreibprüfung unterstützt die amerikanische und die britische Sprache. Wenn Sie eine Mail geschrieben haben, können Sie mit "**Rechtschreibprüfung**" die Rechtschreibprüfung starten. Es erscheint ein blau umrandetes Feld, das den Text der Nachricht enthält. Inkorrekte Wörter sind in rot. Sie können Sie korrigieren, indem Sie die neue Schreibweise eingeben oder einen **Vorschlag** auf der Liste wählen.

- **Ignorieren** – Ein einzelnes rot markiertes Wort wird in dieser Nachricht ignoriert.
- **Alle ignorieren** – Alle Vorkommen des markierten Wortes werden in dieser Nachricht ignoriert.
- **Dem Wörterbuch hinzufügen** – Das markierte Wort wird dem persönlichen Wörterbuch des Benutzers hinzugefügt. Das Wort wird in nachfolgenden Nachrichten nicht mehr als falsch markiert. Die Benutzerwörterbücher werden in den Benutzerpostfächern gespeichert.
- **Ändern** – Ein einzelnes rot markiertes Wort wird in dieser Nachricht geändert.
- **Alle ändern** – Alle Vorkommen eines Wortes werden in dieser Nachricht geändert.
- **Schließen** – Beendet die Rechtschreibprüfung.

Adressbücher

Der Adressbuch-Bereich bietet drei benutzerbezogene Adresslisten:

- **602LAN SUITE-Benutzer** – Diese Liste beinhaltet alle Konten auf dem 602LAN SUITE-Server.
- **Private Listen** – Jeder Benutzer hat eine oder mehrere private Adresslisten. Sie können so viele Listen erstellen, wie Sie möchten.
- **Öffentliche Listen** – Nur ein Benutzer mit Administrator-Rechten kann öffentliche Listen erstellen und ändern.



Kontakte importieren

Kontakte können in private oder öffentliche Listen importiert werden. Um Kontakte zu importieren, aktivieren Sie die Liste in die Sie importieren möchten (entweder privat oder öffentlich) und klicken Sie auf "Importieren":

1. Wählen Sie die zu importierende CSV-Datei.
2. Geben Sie dem neuen Adressbuch einen Namen.
3. Wählen Sie den zu importierenden Adresstyp (alle Adressen, Mail-Adressen, Fax-Adressen).
4. Klicken Sie "OK".
5. Wählen Sie die passenden Zuordnungen und klicken Sie dann "Importieren".

HINWEIS: Nur Administratoren können öffentliche Adressbücher importieren.

Export

Kontakte können in eine CSV-Datei exportiert werden. Um Kontakte zu exportieren, wählen Sie die zu exportierende Liste (entweder privat oder öffentlich) und klicken Sie auf "Exportieren":

1. Wählen Sie, welche Informationen Sie exportieren möchten.
2. Klicken Sie dann "OK".
3. Die CSV-Datei wird an den Webbrowser gesendet und Sie können sie speichern.

Personen finden…

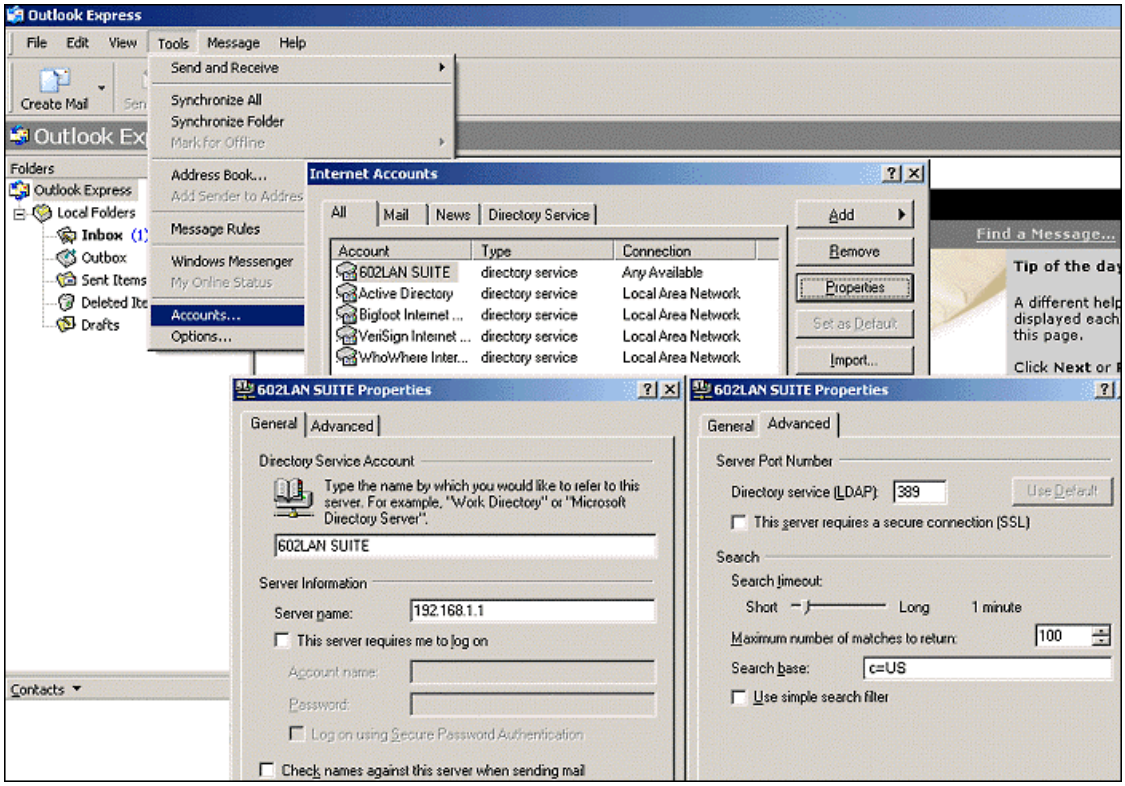
Um Personen zu finden, verwendet 602LAN SUITE die sogenannten Verzeichnis-Dienste (Directory Services). Der 602LAN SUITE Webmail-Client verwendet Verzeichnis-Dienst-Konten, die in Outlook Express definiert wurden und auf dem 602LAN SUITE-Server liegen.

Was sind Verzeichnis-Dienste?

Ein Verzeichnis-Dienst ist ein mächtiges Sucherwerkzeug, das dazu verwendet werden kann Menschen und Unternehmen auf der ganzen Welt zu finden. Das Adressbuch unterstütz LDAP (Lightweight Directory Access Protocol) um Zugang zu den Verzeichnis-Diensten zu bekommen und bietet einen eingebauten Zugang zu verschiedenen, populären Verzeichnis-Diensten. Weitere Verzeichnis-Dienste können Sie von Ihrem Internet-Provider hinzufügen.
Wie andere Internet Suchwerkzeuge verwendet der Verzeichnis-Dienst verschiedene Methoden um Daten zu sammeln. Wenn Sie eine Person oder ein Unternehmen online finden wollen, sollten Sie mehrere Dienste ausprobieren.

Wie man einen 602LAN SUITE Verzeichnis-Dienst

Starten Sie Outlook Express (muss auf dem 602LAN SUITE-Server installiert sein), klicken Sie Werkzeuge/Konten/Hinzufügen/Verzeichnis-Dienste und füllen Sie es, wie das Bild unten zeigt, aus.



Am wichtigsten ist das **Servernamen**-Feld im Allgemein-Register. Es muss die IP-Adresse des Computers, auf dem 602LAN SUITE läuft enthalten und die Suchbasis im **Erweitert**-Register muss die gleiche sein, wie auf dem 602LAN SUITE-Server (Erweiterte Konfigurationen/Benutzer/LDAP-Verzeichnis). Im Zweifelsfall fragen Sie Ihren Administrator.
Nachdem Outlook Express konfiguriert ist, klicken Sie den „**Personen finden**"-Schalter, wählen Sie 602LAN SUITE in dem „**Suchen in**"-Feld. Um eine in 602LAN SUITE definierte Mailadresse zu finden, geben Sie einen Namen oder einen Teil davon ein (z.B. bob), klicken Sie den **Suchen**-Schalter und der 602LAN SUITE-Verzeichnis-Dienst sollte Bob's Mailadresse rausgeben.

Optionen

Oben im Bereich "Optionen" befinden sich vier Schaltflächen:

- **Information** – Zeigt eine Seite mit Benutzer-Informationen.
- **Kennwort** – Hier können Sie Ihr Kennwort ändern.
- **Filterregeln** – Hier können Sie für eingehende Mails Filterregeln definieren.
- **Ich bin abwesend/Ich bin hier** – Diese Schaltfläche aktiviert bzw.. deaktiviert die Anwendung der Filterregeln.
- **Spamschutz-Einstellungen** - Hier werden die Regeln für die Behandlung von SPAM festgelegt.

Optionenmenü

Layout

- **Posteingangszeit anzeigen** – Aktiviert/Deaktivert die Zeitanzeige auf der Posteingangsseite.
- **Zeilenbreite** – Maximale Anzahl von Buchstaben in einer einzigen Zeile.
- **Vorschau der ersten drei Zeilen von ungelesenen Mails** - Aktiviert/Deaktiviert die drei Zeilen-Vorschau.
- **Mails pro Seite** - Anzahl der in einem Ordner auf einmal angezeigten Mails.
- **Internetlinks (URLs) im Dokument hervorheben** - Wenn Sie diese Option auswählen, werden in den Dokumenten alle als Internetlinks erkannten Textstellen als solche markiert. Sie können sie anklicken und die entsprechende Seite öffnet sich in einem neuen Fenster.
- **Mail-Header** - Jede Mail beinhaltet einen Header. Sie können aus drei Headerarten auswählen: Ausführlicher Header, kein Header, kurzer Header.

- **Verzeichnisbaum aktivieren** – Aktiviert den Verzeichnisbaum im Posteingang.

Mail

- **Signaturtext** - Signaturtext, der automatisch an das Ende Ihrer gesendeten Mails gehängt wird.
- **Standardadressbuch** – Wählen Sie das Standardadressbuch, das angezeigt wird, wenn Sie beim Erstellen einer neuen Mail auf “An:” oder “CC:” klicken.
- **Sprache für Rechtschreibprüfung** - Wählen Sie die Standardsprache für die Rechtschreibprüfung.

Postfach

- Kopie jeder versendeten Mail im **Versendete Mails**-Ordner speichern.
- Gelöschte Mails in den **Gelöschte Mails**-Ordner verschieben.

Zip-Unterstützung für Anhänge

- Alle angehängten Dateien bei neuer E-Mail als ZIP-Datei hinzufügen
- Alle angehängten Dateien bei geöffneter E-Mail als ZIP-Datei hinzufügen

HINWEIS: 602LAN SUITE-Webmail erlaubt es, die Anhänge einzeln zu laden oder alle Anhänge als eine ZIP-Datei.

Virenschutz

Der Virenschutz besteht aus zwei Optionen:

- **Dateianhänge neuer Mails scannen** – Jeder Dateianhang einer neuen Mail wird auf Viren überprüft.
- **Dateianhänge geöffneter Mails scannen** - Beim Öffnen einer empfangenen Mail werden alle angehängten Dateien auf Viren geprüft.

Filterregeln

Jede Filterregel besteht aus zwei Teilen:

- Bedingungen, die entscheiden, ob die Regel angewendet werden soll.
- Eine Aktion, die ausgeführt werden soll, wenn die Bedingungen zutreffen.

Klicken Sie auf "Neue Filterregeln hinzufügen", um eine neue Regel hinzuzufügen.

Anwenden

Wählen Sie, wann die Regel angewendet wird:

- Immer
- Nur, wenn ich abwesend bin – Siehe die Schaltfläche im Optionen-Bereich.
- Nur, wenn ich anwesend bin – Siehe die Schaltfläche im Optionen-Bereich.
- Nie

Bedingungen

Hier können Sie Bedingungen definieren, die entscheiden, ob die Regel angewendet wird. Wenn Sie keine Bedingungen definieren, wird die Regel gemäß der Einstellungen bei "Anwenden, wenn" auf alle eingehenden Mails angewandt.

Beispiel 1: Bei dieser Einstellung wird die Regel für alle eingehenden Mails außer Mails von bob@firma.de angewendet.

Beispiel 2: Bei dieser Einstellung wird die Regel nur für eingehende Mails von georg@firma.de verwendet.

Aktion

Wenn eine eingehende Mail zu der Einstellung "Anwenden, wenn" und zu den Bedingungen passt, dann wird die definierte Aktion ausgeführt. Es gibt verschiedene Aktionen:

- **Nichts tun** – Dies können Sie mit "Nach Aktion löschen" dazu verwenden, um eine Regel zu definieren, die bestimmte Mails löscht.
- **In Ordner verschieben** – Wenn Sie im Eingangsordner eigene Ordner definiert haben, können Sie die eingehende Mail in den ausgewählten Ordner verschieben.
- **Weiterleiten** – Sie können eingehende Mails weiterleiten.
- **Antworten** – Antwortet automatisch auf die Mail. Tragen Sie den gewünschten Antworttext ein. *Auf ein Fax kann nicht geantwortet werden.*
- **Benachrichtigen** – Eine Benachrichtigung über die Mail senden.

Hinweise

- Sie können in den Feldern "Absender", "Empfänger" (bei "Bedingungen") sowie "An" und "Kopie" (bei "Aktion/Weiterleiten") nicht mehr als eine Mail-Adresse eingeben. Wenn Sie dies benötigen, erstellen Sie mehrere Regeln.
- Wenn Sie mehr als eine Regel definieren, werden die Regeln von oben nach unten abgearbeitet.
- Wenn das Abarbeiten der Regeln nach einer bestimmten Mail gestoppt werden soll, wählen Sie "Verarbeitung stoppen".
- Wenn Sie einige Regeln temporär deaktivieren möchten, erstellen Sie eine Regel mit der "Nichts tun"-Aktion und verschieben Sie diese über die Regeln, die ignoriert werden sollen.

Spamschutz-Einstellungen

Als Spam bezeichnet man unerwünschte Mails die an eine große Anzahl von Leuten geschickt wird um Werbung für ein bestimmtes Produkt oder eine Dienstleistung zu machen.

Optionen

Prüfmethoden:

- **Positiv-/Negativlisten zum Prüfen ankommender Mails verwenden** – Schaltet die Funktionalität der Positivliste (alle Mails von der Liste kommen an) und Negativliste (alle Mails von der Liste werden abgelehnt) ein.
- **Absender werden nach Klassifizierung automatisch auf die Positiv-/Negativliste gesetzt** – Je nachdem, ob Sie den Absender als Spam oder als nicht Spam klassifizieren.

Mailmarkierung

Ankommender Spam wird wie folgt markiert:

- **Folgenden Betreff zur Mail hinzufügen –** Geben Sie den Text ein, der an das Nachrichten Thema gehängt wird und wählen Sie die Markierungs-Position (am Anfang oder am Ende des Themas).
- **X-LNS-Spamprüf-Header zur Mail hinzufügen** – Fügt dem Kopfteil detaillierte Informationen über die Spam-Mail hinzu.

SPAM-Mailaktionen

Wenn eine ankommende Mail eine Spam-Mail ist, bietet der Web-Mail Client folgende Aktionen an:

- **In Ordner xxx verschieben –** Wählen Sie den Ordner in den die Spam-Mail verschoben wird. Standardmäßig ist dies der Nachrichten Eingang.
- **In Ordner xxx erstellt unter xxx verschieben –** Geben Sie den Ordnernamen für die Spam-Mail ein, der dann als Unterordner des gewählten Ordners erstellt wird.
- **Löschen –** ankommende Spam-Mail wird automatisch gelöscht.

Positiv-/Negativliste

602LAN SUITE bietet zwei Kontrolllisten:

- **Positivliste (Whitelist) –** Nachrichten von diesen Absendern werden NIE als Spam klassifiziert.
- **Negativliste (Blacklist) –** Nachrichten von diesen Absendern sind Spam.

Sie können jedes Objekt der Liste hinzufügen, löschen oder bearbeiten. Eine Liste mit Mail Adressen von einer .CSV-Datei kann ebenfalls **importiert** werden.

Automatisches Hinzufügen zur Positivliste
Diese beiden Optionen schalten das automatische Hinzufügen von Mail Adressen auf die Positivliste an bzw.. aus:

- **Empfänger der von Ihnen versendeten Mails hinzufügen –** Es sollte davon ausgegangen werden, dass ein Empfänger dem Sie Mail senden jemand ist, dessen Mails Sie auch erhalten wollen. Bei Aktivierung dieser Option wird der Empfänger also automatisch der Whitelist hinzu gefügt.
- **Empfänger der von Ihnen erhaltenen KEIN-SPAM-Mails hinzufügen –** Wenn Sie eine Nachricht als nicht Spam klassifizieren, werden alle weiteren Empfänger (im AM- oder CC- Feld) automatisch auf die Whitelist gesetzt.

WAP-Zugriff

602LAN SUITE bietet über das WAP-Protokoll (Wireless Access Protocol) auch für drahtlose Geräte Zugriff auf den Webmail-Client. Die meisten internetfähigen Handys und einige PDAs unterstützen dieses Protokoll.

Voraussetzungen

- Ein internetfähiges Telefon, das das WAP-Protokoll unterstützt (Wireless Access Protocol). Die meisten internetfähigen Telefone unterstützten dieses Protokoll.
- Einen Internetanbieter für Ihr Telefon.
- Eine Internet-Verbindung für 602LAN SUITE mit einer statischen IP-Adresse, einem statischen Domänen-Namen oder dynamischen DNS-Dienst.

Einrichtung

Wir können wegen der Unterschiede bei der Einrichtung verschiedener Telefone keine spezifischen Anweisungen, wie sich bestimmte Telefone konfigurieren lassen, geben. Bitte verwenden Sie die folgenden Schritte als Referenz anstatt als exakte Anweisungen. Lesen Sie das Handbuch Ihres Telefons oder fragen Sie dessen Hersteller für weitere Hilfe. Zusätzliche Informationen zu WAP finden Sie auf http://www.yourwap.com/.

1. Gehen Sie auf Ihrem Telefon zu den Favoriten.
2. Fügen Sie einen neuen Favoriten hinzu und geben Sie ihm einen Namen wie "EMAIL".
3. Als URL geben Sie die Web-Adresse Ihres 602LAN SUITE-Servers an und fügen Sie am Ende "/wap" hinzu. Wenn Sie eine Internet-Verbindung mit statischer IP-Adresse verwenden, sollte Ihre URL wie "http://206.182.14.251/wap" oder "http://www.ihre-firma.de/wap" aussehen.
4. Speichern Sie Ihren neuen Favoriten.

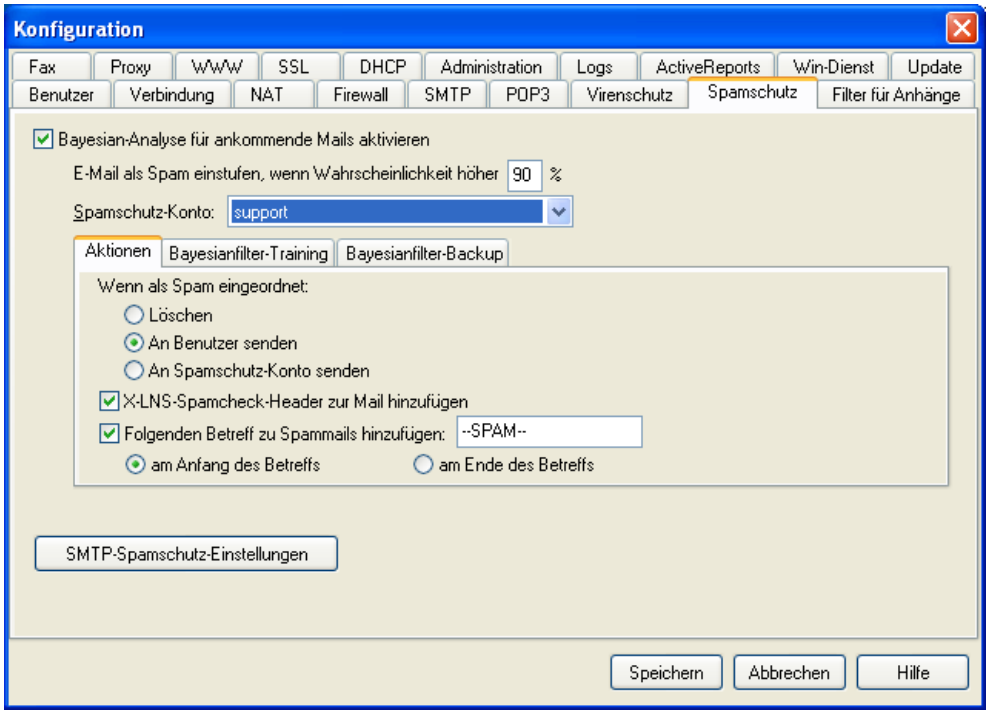
Spamschutz

602LAN SUITE bietet vier Arten des Spamschutzes an:
602LAN SUITE SMTP lehnt ankommende Nachrichten sofort/nie ab:

- **DNSBL-Service** – 602LAN SUITE kann Nachrichten in Bezug auf die Antwort einer Anfrage an einen DNS Lookup-Service ablehnen. Diese Dienste speichern die Adressen bekannter Spam-Domänen.
- **SMTP-Server-Positiv-/Negativliste (Whitelist /Blacklist)** – 602LAN SUITE kann Mails ablehnen, die von einem Host/Absender kommen, der in der Negativliste (Blacklist) eingetragen ist. Mails von einem Host/Absender, der in die Positivliste (Whitelist) eingetragen ist, werden nie abgelehnt. Diese globale Liste ist für alle 602LAN SUITE-Benutzer gleich.

Ankommende Nachrichten werden immer akzeptiert. Im Betreff bzw. im Header der Mail wird eine Markierung eingefügt, die nach den Einstellungen behandelt wird:

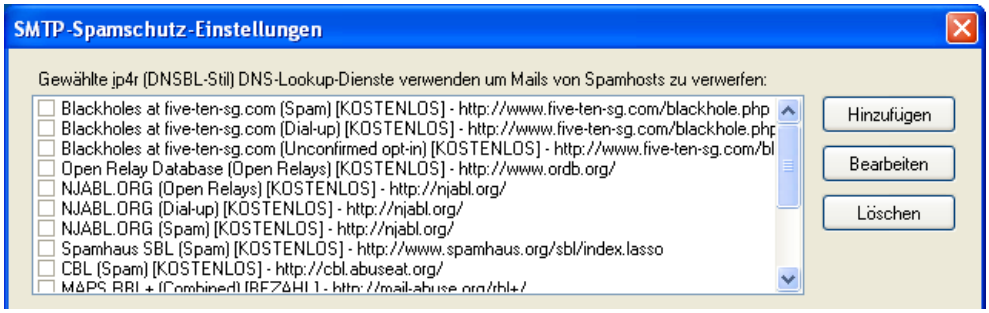
- **Bayesian-Filter** – Die Bayesian-Spam-Filterung ist ein erweiterter Inhalt-Klassifizierungs-Filter. 602LAN SUITE kann Spam-Mail erkennen und auf der Basis einer vorhergehenden Klassifizierung von SPAM- bzw. KEIN SPAM-Mails eine ausgewählte Aktion durchführen.
- **Persönliche Postiv-/Negativliste** – Diese Listen sind persönliche Benutzer-Listen, die vom 602LAN SUITE Webmail-Client aus verwaltet werden können. Jeder Benutzer hat seine persönlichen Listen.



Schutz mit DNS-Negativlisten (DNS-BL)

Spamschutz durch DNS-Ausschlusslisten (auch Blacklist oder DNS-bl genannt) ist ein gemeinschaftlicher Ansatz von Internetanbietern, bekannten Spam-Domänen den Zugriff auf Mail-Dienste (SMTP) zu verweigern. Einige bieten diesen Dienst kostenlos an (Schlüsselwort "[kostenlos]", "[FREE]"), andere nicht ("[bezahlt]", "[PAY]"). Die Spamschutz-Einstellungen finden Sie unter "SMTP/Spamschutz-Einstellungen". Es gibt verschiedene Arten von Spamschutz-Datenbanken:

- **Spam** – Enthält bestätigte Spammer. Sehr empfehlenswert.
- **Einwahl-Zugänge** – Enthält dynamisch zugewiesene IP-Adressen. Empfehlenswert.
- **Offene Relays** – Enthält ungesicherte Mail-Server, die Mails von jedem annehmen. Sehr empfehlenswert.
- **Kombiniert** – Kombination der ersten drei Arten.


SMTP-Spamschutz-Einstellungen
Gewählte ip4r (DNSBL-Stil) DNS-Lookup-Dienste verwenden um Mails von Spamhosts zu verwerfen:
Blackholes at five-ten-sg.com (Spam) [KOSTENLOS] - http://www.five-ten-sg.com/blackhole.php
Blackholes at five-ten-sg.com (Dial-up) [KOSTENLOS] - http://www.five-ten-sg.com/blackhole.php
Blackholes at five-ten-sg.com (Unconfirmed opt-in) [KOSTENLOS] - http://www.five-ten-sg.com/bl
Open Relay Database (Open Relays) [KOSTENLOS] - http://www.ordb.org/
NJABL.ORG (Open Relays) [KOSTENLOS] - http://njabl.org/
NJABL.ORG (Dial-up) [KOSTENLOS] - http://njabl.org/
NJABL.ORG (Spam) [KOSTENLOS] - http://njabl.org/
Spamhaus SBL (Spam) [KOSTENLOS] - http://www.spamhaus.org/sbl/index.lasso
CBL (Spam) [KOSTENLOS] - http://cbl.abuseat.org/
Hinzufügen
Bearbeiten
Löschen

Um einen Dienst hinzufügen, wählen Sie diesen und klicken Sie auf "Hinzufügen". Um einen Dienst zu bearbeiten, klicken Sie auf "Bearbeiten".

- **Dienstname** – Beschreibender Name eines DNS-Lookup-Spamschutz-Anbieters.
- **DNS-Lookup-Domäne** – Die Domäne, über die der Dienst angesprochen wird.
- **IP-Adresse für aufgeführte Hosts zurückgeben** – Der Spamschutz-Anbieter liefert die IP-Adresse zurück, wenn der Host in der Spamschutz-Datenbank gefunden wird.
- **Antworten, wenn abgewiesen** – Definiert die zu sendende Nachricht, wenn die Mail von einer Spam-Domäne kommt.

Um einen Dienst zu löschen, klicken Sie auf "Löschen".

Schutz mit der SMTP Positiv-/Negativliste

Wenn Sie die SMTP-Server-Positivliste (Whitelist) und -Negativliste (Blacklist) definieren wollen, klicken Sie das SMTP-Register, dann den Schalter für die SMTP Spamschutz-Einstellungen. Der 602LAN SUITE-SMTP-Server lehnt sofort ankommende Nachrichten gemäß dieser Listen ab.

Dort können Sie spezielle Absender oder Hosts eingeben, von denen Sie keine Mails akzeptieren (Negativliste) oder von denen Sie Mails akzeptieren (Positivliste) wollen. Es ist möglich einzelne Einträge zu bearbeiten oder zu löschen. Spezielle Absender oder Hosts können von/in eine Datei importiert/exportiert werden. Die Datei muss eine reine Textdatei sein, mit jeweils nur einem Absender/Host pro Zeile.

- **Host** – Ein Host ist der Mailhost des Absenders. Wenn der Mailhost für die Mailadresse bob@firma.de ist, geben Sie firma.de ein.
- **Absender** – Der Absender ist die ganze Mailadresse des Absenders. Um bob@firma.de zu zulassen/abzulehnen, geben Sie bob@firma.de ein. Um ALLE Adressen von firma.de zu zulassen/abzulehnen geben Sie *@firma.de ein.

Anmerkung: Ein Host kann Mails für mehrere Domänen versenden. So kann es passieren, dass Sie die Mails von mehr als einer Domäne blocken.

Schutz mit dem Bayesian-Filter

Technische Beschreibung des Bayesian-Filters: http://spambayes.sourceforge.net/ .

Aufbau

Der Aufbau des Bayesian-Systems ist in klare Teile gegliedert. Der Erste und Offensichtlichste ist das Inhaltsprogramm, das Mails auffängt und in Wortserien aufgliedert. In diesem Moment nimmt es Worte aus dem

Textteil der Nachricht, entfernt den HTML-Kode und andere, nicht benötigte Informationen (z.B. Bilder). Gleichzeitig wird der Kopfteil der Mail interpretiert, während eine interne Verarbeitung vonstatten geht.

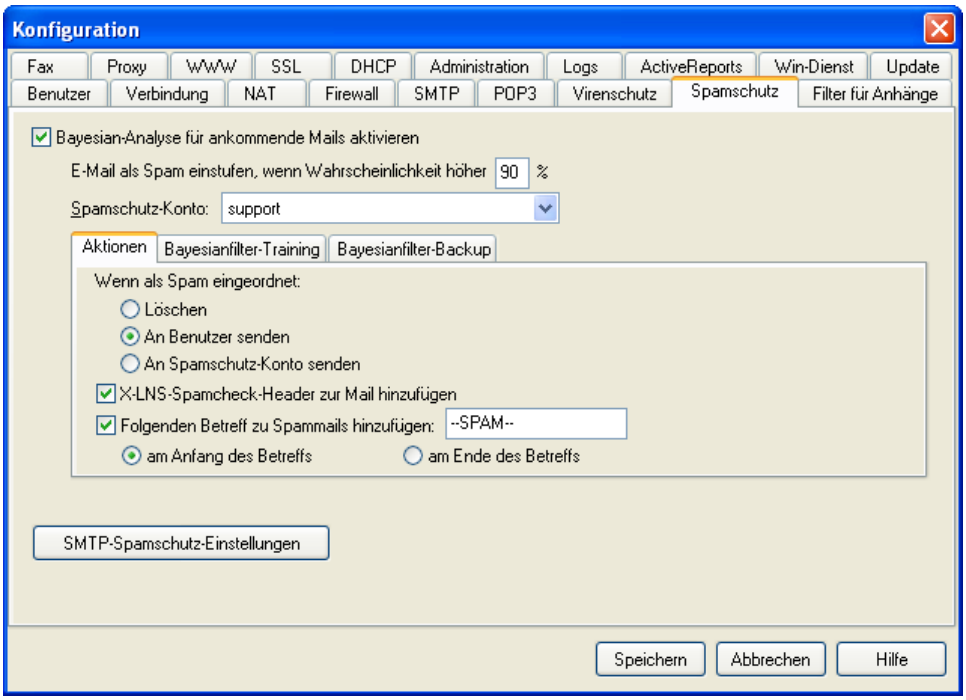
SPAM und KEIN SPAM

Der Bayesian-Filter versucht ankommende Mails in Spam und kein Spam zu unterteilen. Das bedeutet, dass Spam-Mails automatisch in einen extra Ordner sortiert werden können.

Als Erstes muss der Bayesian-Filter trainiert werden, zwischen Spam und nicht Spam zu unterscheiden. Grundsätzlich beginnen Sie damit ihm eine Reihe von Mails zu zeigen, die Spam bzw. kein Spam sind. Der Filter analysiert daraufhin die Mails um Anhaltspunkte zur Unterscheidung zu finden. Z.B. verschiedene Worte, Unterschiede im Header und im Inhaltsstil. Das System verwendet diese Anhaltspunkte um neu ankommende Mails zu untersuchen.

Der 602LAN SUITE-Bayesianfilter

Der 602LAN SUITE-Bayesian-Filter klassifiziert die ankommenden Mails und schreibt das Ergebnis in den Header. Wenn eine Mail als Spam erkannt wurde, kann 602LAN SUITE (je nach Einstellungen) einen Text in den Mail-Betreff und eine Punktewertung in den Header eintragen.



602LAN SUITE-Bayesianfilter trainieren

Benutzer haben dazu verschiedene Möglichkeiten:

- **Webmail** – Benutzer können ankommende Mails klassifizieren, indem Sie auf das SPAM bzw. KEIN SPAM-Symbol im Posteingang klicken.
- **POP3-Client** – Benutzer können ankommende Mails klassifizieren, indem Sie die Mails an die entsprechende Adresse weiterleiten: junk@junk für SPAM oder notjunk@junk für KEIN SPAM.
- **Persönliche Positivliste** – Es ist möglich die Option „Automatisch mit Absendern in der Positivliste trainieren“ auszuwählen, die Sie im „Bayesianfilter-Training“-Register finden. Diese Nachrichten trainieren den Filter dann automatisch.

Bayesianfilter-Aktionen

Wenn der 602LAN SUITE Bayesian Filter eine Mail als Spam klassifiziert, können Sie aus drei möglichen Optionen wählen:

- **Löschen** – Löscht die Nachricht sofort
- **An Benutzer senden** – Sendet die Nachricht an den Benutzer
- **An Spamschutz-Konto senden –** Sendet die Mail zur weiteren Verarbeitung zum Spamschutz-Konto.

Unabhängig von den Aktionen können Sie folgenden Optionen definieren:

- X-LNS Spam-Check-Header zur Mail hinzufügen

- Folgenden Betreff zu Spammails hinzufügen

Bayesianfilter-Training

- Wählen Sie die Option „Automatisch mit Absendern der Positivliste trainiere“ an. Der 602LAN SUITE-Bayesian-Filter verwendet Mails von diesen Absendern um sich selbst zu trainieren.
- Wählen Sie eine Methode wie das Update des Bayesian-Filters vollzogen wird, wenn Benutzer Mails als SPAM oder KEIN SPAM klassifizieren.

Bayesianfilter-Backup

Die 602LAN SUITE–Bayesian-Datenbank kann jederzeit gespeichert werden. Wir empfehlen eine Datensicherung um ein falsches Training, das z.B. durch die falsche Einordnung von Mails zustande gekommen ist, wieder rückgängig zu machen. In diesem Fall können Sie einfach eine ältere Datenbank wieder herstellen.

602LAN SUITE-Spamschutz-Konto

Das Spamschutz-Konto kann jedem 602LAN SUITE-Benutzer zugewiesen werden, aber wir empfehlen ein spezielles Konto für Spam-Mails einzurichten.

Wie arbeitet das Spamschutz-Konto?

Mails, die als Spam klassifiziert wurden, werden an dieses Konto geschickt.

Der Administrator oder jeder, der den Login-Namen und das Passwort besitzt, kann in diesem Konto regelmäßig nach falsch klassifizierten Mails schauen.

- Je nach den Bayesianfilter-Einstellungen wird eine Nachricht an dieses Konto gesendet, dass der Filter aktualisiert wurde **ODER** es wird eine Anfrage gesendet, ob der Filter aktualisiert werden soll.

Schutz durch persönliche Positiv- und Negativliste

Jeder Benutzer hat eine eigene Positiv- und Negativliste. Um diese persönlichen Listen zu definieren, starten Sie den 602LAN SUITE Webmail-Client, klicken Optionen und dann den Schalter für die Spamschutz-Einstellungen.

Hier können Sie Absender oder Hosts eingeben, von denen Sie Mails (Positivliste/Whitelist) bzw. keine Mails (Negativliste/Blacklist) empfangen möchten. Sie können einen einzelnen Eintrag ändern oder löschen. Die gewählten Absender oder Hosts können importiert oder exportiert werden. Das Dateiformat hierfür ist einfacher Text mit einem Absender oder Host pro Zeile.

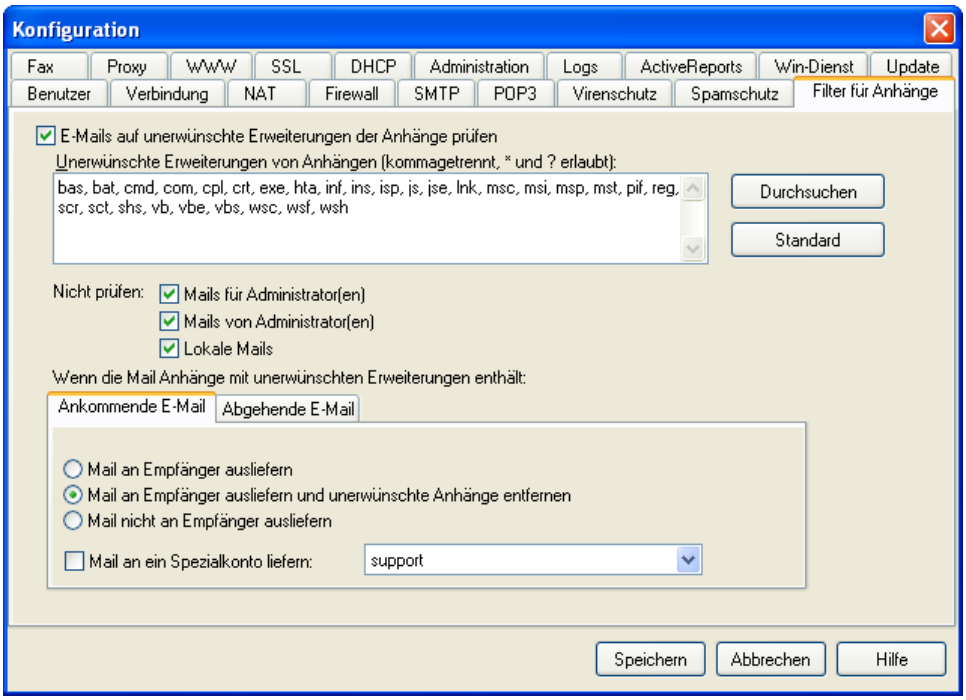
- **Host** - Ein Host ist der Host für den Mail-Server des Absenders. Wenn die Mail von "spammer@spamhafen.de" über den Mail-Host "mail.spamhafen.de" verschickt wird, geben Sie "mail.spamhafen.de" ein.
- **Absender** - Das ist die komplette Mail-Adresse des Absenders. Um nur "spammer@yahoo.de" abzuweisen/zu erlauben, geben Sie "spammer@yahoo.de" ein. Um alle Adressen von "spammen.de" abzuweisen/zu erlauben, geben Sie "*@spammen.de" ein.

Hinweis: Ein Host kann für mehrere Domänen Mails verschicken. So blockieren Sie möglicherweise Mail von mehr als einer Domäne.

Filter für Anhänge

Ankommende/Abgehende Mails können angehängte Dateien enthalten. Es ist möglich Dateiendungen zu definieren, die von 602LAN SUITE überprüft werden. Nachrichten die diese Anhänge enthalten werden je nach Einstellung wie folgt behandelt:

- **Mails auf unerwünschte Erweiterungen der Anhängen prüfen** – Schaltet den Anhangsfilter an bzw. aus.
- **Unerwünschte Erweiterungen von Anhängen** – Geben Sie hier die Endungen der angehängten Dateien ein, die vom Filter bearbeitet werden.
- **Nicht prüfen** – Aktivieren Sie diese Option, wenn Sie Mails von/für die Administratoren oder lokale Mails nicht prüfen wollen.
- **Ankommende/Abgehende E-Mail** – Hier können Sie eine Aktion für einen ungewollten Anhang festlegen.

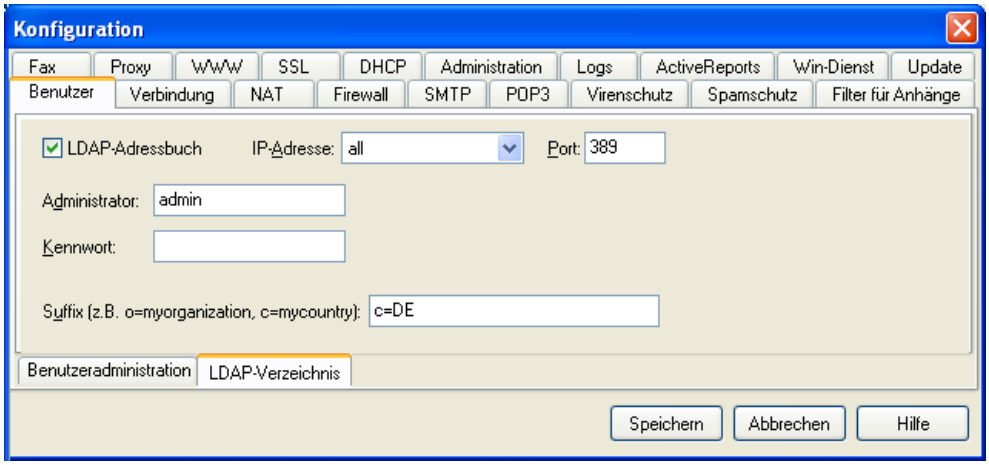


Einrichtung des LDAP-Adressbuchs

LDAP

Um das LDAP-Adressbuch von 602LAN SUITE zu verwenden, wählen Sie das Hauptregister „Benutzer“ und aktivieren dort im Unterregister "LDAP" oben links die Option "LDAP-Adressbuch".

- **IP-Adresse -** Wenn der Computer, auf dem 602LAN SUITE läuft, als Internet-Gateway arbeitet und über zwei Netzwerk-Adapter verfügt, haben Sie mehrere Möglichkeiten:
  - **Wählen Sie die IP-Adresse des internen Netzwerks** – Benutzerinformationen sind nur vom internen Netzwerk aus zugänglich.
  - **Wählen Sie die IP-Adresse des externen Netzwerks** – Benutzerinformationen sind nur vom externen Netzwerk aus zugänglich (vom Internet aus).
  - **Wählen Sie alle Netzwerk-Schnittstellen** – Benutzerinformationen sind vom Internet und dem lokalen Netzwerk aus zugänglich.
- **Port:** Der Standardport für LDAP ist 389. Wenn Sie diesen Wert ändern, müssen die die LDAP-Clients (Mail-Programme) auch entsprechend umkonfigurieren.



Microsoft® Outlook Express als LDAP-Client einrichten

Sie können Outlook Express wie folgt als LDAP-Client einrichten:

1. Wählen Sie "Adressbuch" aus dem "Extras"-Menü.
2. Wählen Sie im Adressbuchfenster "Konten" aus dem "Extras"-Menü.
3. Klicken Sie im Fenster "Internetkonten" auf "Hinzufügen", um ein neues Verzeichnis hinzuzufügen.
4. Geben Sie als "Verzeichnisdienstserver (LDAP)" den Hostnamen oder die IP-Adresse Ihres 602LAN SUITE-Servers (möglicherweise 192.168.1.1) ein und klicken Sie auf "Weiter".
5. Wählen Sie "Ja" und klicken Sie "Weiter".
6. Klicken auf "Fertig stellen".
7. Der neue Name des neuen Verzeichnisdienstes erscheint alphabetisch einsortiert in der linken Spalte.
8. Wählen Sie den Verzeichnisdienst, den Sie erstellt haben und klicken Sie "Eigenschaften".
9. Aktivieren Sie das Register "Erweitert".
10. Geben Sie als "Suchbasis" an, was im Konfigurationsfenster von 602LAN SUITE im Register "LDAP" unter "Suffix" angegeben ist, zum Beispiel "c=DE" für Deutschland. Klicken Sie dann auf "OK" und dann auf "Schließen", um das Fenster "Internetkonten" zu schließen.
11. Klicken Sie nun im Adressbuchfenster "Personen suchen" an.
12. Wählen Sie vom Ausklappmenü "Suchen in" den neuen Verzeichnisdienst.
13. Aktivieren Sie das Register "Erweitert".
14. Wählen Sie bei "Kriterien festlegen" "Mail" "enthält", geben Sie das Klammeraffen-Symbol "@" ein und klicken Sie auf "Hinzufügen".
15. Klicken Sie nun "Suche starten", um alle Benutzer in der 602LAN SUITE-Benutzerliste anzuzeigen.

Praktischer Nutzen von LDAP

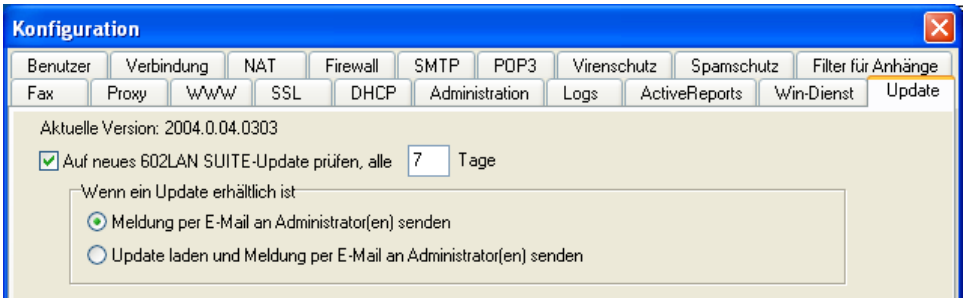
Benutzer, die einen Mail-Client verwenden, der LDAP unterstützt (z.B. Outlook Express), können Adressen aus dem LDAP-Verzeichnis importieren. Der LDAP-Client nimmt Verbindung mit dem LDAP-Server von 602LAN SUITE auf und übernimmt alle Mail-Adressen aus dem 602LAN SUITE-Adressbuch auf. Dieses enthält alle Mail-Adressen der im Register "Benutzer" eingerichteten Benutzer, deren Mail-Benutzer für das LDAP-Adressbuch freigegeben sind.

602LAN SUITE Update Manager

602LAN SUITE kann automatisch nach neuen Updates suchen. Wollen Sie dies, so schalten Sie die Option „Nach neuen 602LAN SUITE Updates suchen, alle x Tag(e)“ ein.

Wenn ein 602LAN SUITE Update verfügbar ist, wählen Sie eine der folgenden Optionen:

- **Meldung per E-Mali an Administrator(en) senden** – Eine Update-Benachrichtigung wird an alle Administratoren geschickt.
- **Update laden und Meldung per E-Mail an Administrator(en) senden** – Das neue Update wird herunter geladen und eine Benachrichtigung an alle Administratoren geschickt.



Wenn Sie die Zeit begrenzen wollen, in der das Update herunter geladen wird, wählen Sie die „Updatezeit“-Option an und geben Sie die gewünschte Zeit ein. Das Standardzeit-Interval ist von 00:00 – 5.00.
Wenn 602LAN SUITE per Einwahlverbindung mit dem Internet verbunden ist und Sie automatisch eine Verbindung für das Herunterladen des Updates herstellen wollen, wählen Sie „Einwahlverbindung für Update-Download aufbauen“.
Wenn Sie einen Proxy-Server benötigen um den Update-Server zu kontaktieren, dann tragen Sie hier die HTTP-Proxy-Adresse ein.

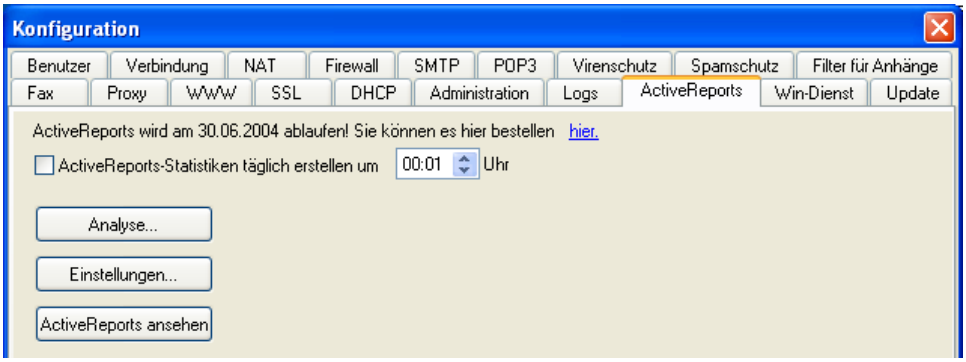
Updatezeit nur von 00:00 bis 05:00
Einwahlverbindung für Update-Download aufbauen
HTTP-Proxy für Kommunikation mit Updateserver:

Wenn Sie die automatische Option nicht verwenden möchten, können Sie den Update-Server auch manuell nach neuen 602LAN SUITE-Updates überprüfen, indem den Sie auf „Updateprüfung“ klicken.

Die alte Version von 602LAN SUITE wird automatisch gespeichert. Wenn während des Starts der neuen Version Fehler auftreten, wird die alte Version wieder hergestellt.

ActiveReports

ActiveReports ist eine 602LAN SUITE-Erweiterung zur Analyse der 602LAN SUITE-Logdateien. ActiveReports erstellt individuelle Statistik-Seiten (HTML) für jeden LAN-Arbeitsplatz und für das ganze LAN. Die Daten werden in Diagrammen für Jahre, Monate oder Tage angezeigt. Sie können sich auch die Werte für Filterergebnisse in Abhängigkeit zu den verschiedenen Protokollen (HTTP, SOCKS usw.) ausgeben lassen. Schalten Sie die Option „ActiveReports-Statistiken täglich erstellen um xxx Uhr“ ein und ActiveReports startet jeden Tag um die angegebene Uhrzeit. Sie können die Analyse auch manuell starten. Für weitere Informationen lesen Sie bitte die ActiveReports-Hilfe.



ActiveReports läuft mit voller Funktionalität 30 Tage als Testversion. Um die Anwendung weiterhin zu verwenden müssen Sie ActiveReports käuflich erwerben.

Arbeitsweise

ActiveReports startet täglich zu einer festgelegten Zeit und analysiert die Protokolldateien (Logs) vom Vortag. Nach der Analyse erstellt ActiveReports statische HTML-Seiten für jeden LAN-Arbeitsplatz. Diese Statistiken sind unter http://www.firma.de/stats/ verfügbar und werden je nach anfragendem Host konfiguriert.

Die Statistiken für das gesamte LAN sind unter http://www.firma.de/admin/stat/ verfügbar. Man braucht dafür einen Administrator-Zugang. Die übertragenen Daten werden in Grafiken nach Jahren, Monaten und Tagen dargestellt. Sie können die Ergebnisse als Gesamtwert oder aufgeteilt nach bestimmten Protokollen (HTTP, SOCKS usw.) anzeigen.

Um detaillierte Informationen zu erhalten (um geladene Dateien, empfangen/versendete Mails usw. zu sehen), starten Sie ActiveReport im interaktiven Modus (602LAN SUITE/Statistiken/ActiveReports/Analyse...) mit dem gewünschten Zeitbereich. Die Daten können im Excel-Format (.csv) und die Grafiken im GIF und BMP-Format gespeichert werden.

Inhaltsfilter (Content Filter)

Der Schutz von Kindern, jungen Menschen, Studenten und Angestellten vor schädlichen und verletzenden Inhalten des Internets wird mehr und mehr eine wichtige Angelegenheit. Das Internet wächst rasant und es gibt nur wenige Kontrollmechanismen über den Inhalt, zumal dies den Interessen mächtiger Organisationen, wie z.B. der pornografischen Industrie, entgegensteht.

Durch die dynamische Natur des Internets sind spezielle Filterwerkzeuge nötig, die mit der Geschwindigkeit des Wachstums und der Änderungen mithalten können. Letztlich hat dabei nur ein dynamischer Inhaltsfilter eine Chance, diese Anforderungen jetzt und in Zukunft zu erfüllen.

Der PureSight Content Filter, der in 602LAN SUITE integriert wurde, vereint zuverlässige Internetfilterung mit einem umfangreichen Verwaltungswerkzeug um eine sehr genaue und verlässliche zu gewährleisten.

Filtermethoden

Es gibt zwei prinzipielle Methoden um Webinhalte während des Browsens im Internet zu identifizieren und zu filtern: URL-Datenbanken und dynamische Inhaltsanalyse.

Statische URL Filterung: URL-Datenbanken

In URL-Sammlungen wird jeder enthaltenen URL eine bestimmte Inhaltskategorie zugeordnet. Wenn eine Site angefordert wird, prüft der Filter die Adresse der angefragten Website in der Datenbank. Gemäß der vom Anwender eingestellten Internet-Nutzungsvorgabe kann der Filter die Seite blockieren oder zulassen.

URL-Datenbanken werden von den Filterherstellern erstellt und gepflegt. Updates werden gewöhnlich auf Abonnementbasis angeboten. Die Datenbank enthält Einträge für Internet-Domainnamen und spezielle Subdomains. Jeder Eintrag wird einer Inhaltskategorie zugeordnet, z.B. Drogen, Glücksspiel, Hass, Pornografie und viele andere. URLs, die in der Datenbank nicht gefunden werden, werden in der Regel durchgelassen.

Dynamische Filterung - Artificial Content Recognition (ACR)

Jede Webseite, die von einem Benutzer angefordert wird, wird Paket für Paket empfangen und zum HTML-Parser geschickt. Der Parser ist die erste Komponente der ACR und er zerlegt den HTML-Code in Hunderte von Parameter und erstellt daraus den Raw Data Vector (RDV). Dabei werden die auf der Webseite befindlichen Wörter, das grundlegende Layout und das Format der Seite miteinbezogen. Nachfolgend einige der Parameter, die in die Analyse einfließen:

Nicht-Text-Informationen:

- **Hintergrundfarbe**
- **Schriftart**
- **Schriftfarbe**
- **Schriftgröße**
- **Anzahl der Links**
- **Anzahl der Bilder**
- **Größe der Bilder**
- **Anzahl der Frames**
- **Durchschnittliche Wortlänge**
- **Anzahl der Wörter**
- **Spezielle Zeichen**
- **Metatags**

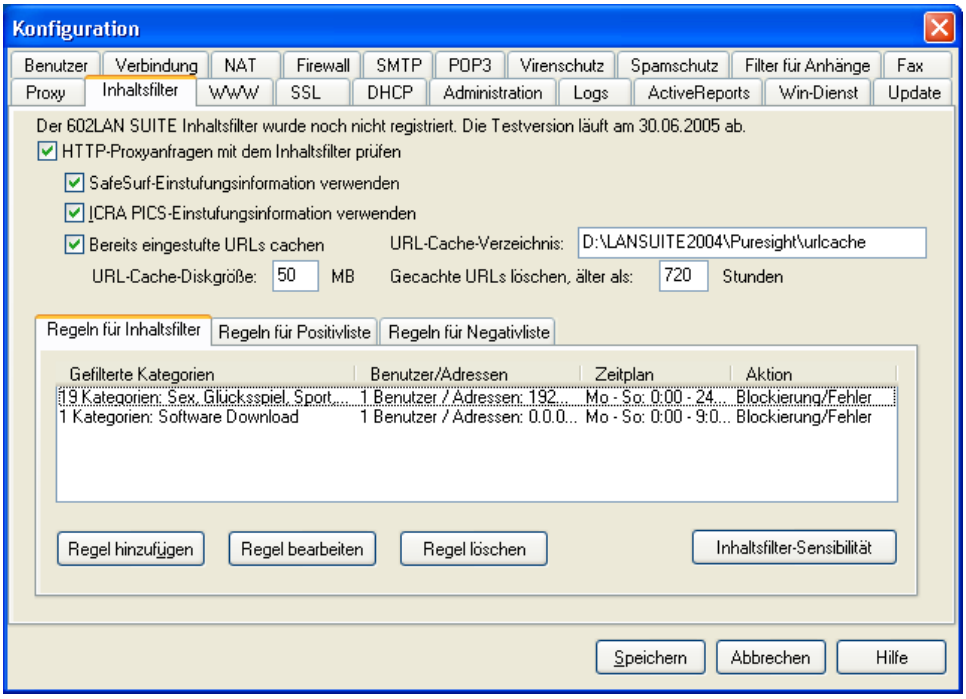
Textinformationen:

- **URL-Name**
- **Metatag-Text**
- **Wörterbuchwörter**

Die ACR-Technologie verwendet eine einstufige Kontrolle, die jedes Paket direkt bei der Ankunft analysiert und nicht warten muss, bis die ganze Seite geladen wurde. Der Vorgang ist dadurch sehr schnell und führt zu keiner nennenswerten Verzögerung beim Benutzer. Zudem wird ein URL-Cache verwendet, der die

Einstufungen der zuvor angeforderten Webseiten zwischenspeichert. Der URL-Cache steigert die Performance und reduziert die Wartezeit, indem er eine dynamische Datenbank erstellt, die den tatsächlichen Surfgewohnheiten des Benutzers oder der Organisation entsprechen. Diese Datenbank enthält daher keine irrelevanten Daten und unterscheidet sich damit von der statischen URL-Datenbank. PureSight vereint damit die Effizienz einer Datenbanklösung durch Verwendung des URL-Caches und reduziert geleichzeitig die Wartezeiten durch das Ausschließen irrelevanter Daten aus dem Cache.

Konfiguration



Aktivierung

Zur Aktivierung der Inhaltsfilterung in 602LAN SUITE muss zuerst die Option ‘HTTP-Proxyanfragen mit dem Inhaltsfilter prüfen’ aktiviert werden.

SafeSurf-Einstufungsinformation verwenden

SafeSurfs Bewertungsstandard ‘PICS’ ist ein Internetprotokoll, das Bewertungen überträgt und internetweit verstanden wird. SafeSurf entwarf PICS (Platform for Internet Content Selection) zusammen mit 22 anderen Firmen (Microsoft, Netscape, AT&T usw.). Im Grunde erlaubt PICS den Inhaltsanbietern, ihre Seiten einzustufen und beispielsweise Eltern, Beschränkungen für ihre Kinder festzulegen. Weitere Informationen unter: http://www.safesurf.com

ICRA PICS-Einstufungsinformation verwenden

Die Internet Content Rating Association (ICRA) ist eine internationale, gemeinnützige Organisation, die daran arbeitet, das Internet sicherer zu machen. Das Herzstück der Organisation ist der beschreibende Wortschatz, oft auch als "der ICRA-Fragebogen" bezeichnet. Inhaltsanbieter prüfen, welche der 45 Elemente des Fragebogens für ihre Website zutreffen oder nicht zutreffen. Daraus wird dann einen Code erzeugt, der als ICRA-Kennzeichen bekannt ist und den der Webmaster auf seine Site stellt. Weitere Informationen unter:http://www.icra.org

Bereits eingestufte URLs cachen

Hiermit kann der Aufbau einer dynamischen Datenbank zur Inhaltsfilterung aktiviert werden. Die Aktivierung wird sehr empfohlen. Die maximale Größe der Datenbank wird bei ‘URL-Cachegröße’ festgelegt.

URL-Cachegröße

Die Größe der Datenbank zur Speicherung klassifizierter URLs in MB.

URL-Cache-Verzeichnis

Hier können Sie das Verzeichnis für die dynamische Inhaltsfilter Datenbank angeben. Es wird empfohlen, das Standardverzeichnis zu belassen.

Gecachete URLs löschen, älter als

Gespeicherte URLs werden gelöscht, wenn sie älter als das Limit sind. Dies ist sinnvoll, weil sich der Inhalt einer URL ändern kann.

Regeln für Inhaltsfilter, Positiv- und Negativlisten

Sie müssen zumindest eine Regel in einem der drei Register eingeben, damit der Inhaltsfilter arbeiten kann.

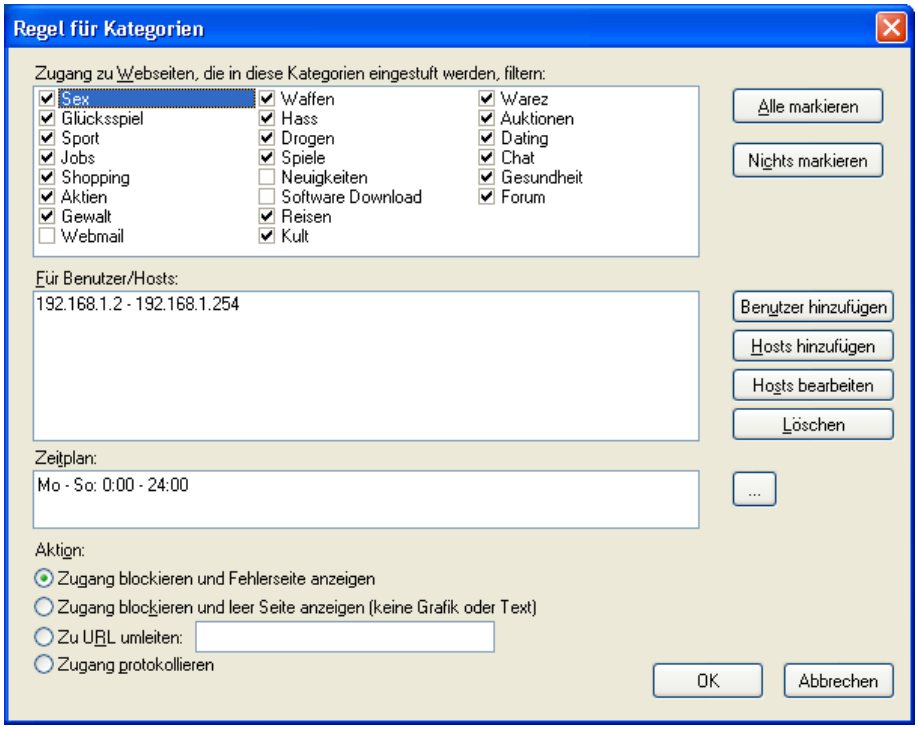
602LAN SUITE verarbeitet die Regeln in der folgenden Reihenfolge:

1. IP-Filter (Proxy-Register)
2. Sitezugriff-Regel (Proxy-Register)
3. Positivliste (Inhaltsfilter-Register)(wenn die URL gefunden wird, werden die nächsten Schritte nicht mehr ausgeführt und die URL wird angezeigt)
4. Negativliste (Inhaltsfilter-Register) (wenn die URL gefunden wird, werden die nächsten Schritte nicht mehr ausgeführt und die URL wird blockiert)
5. Inhaltsfilter (Inhaltsfilter-Register)

Die Regeln werden in den folgenden Registern definiert:

- Positivliste – diese URLs werden immer erlaubt.
- Negativliste – diese URLs werden immer abgelehnt/blockiert.
- Inhaltsfilter - alle URLs, die den Kriterien entsprechen, werden entsprechend der gewählten Aktion behandelt.

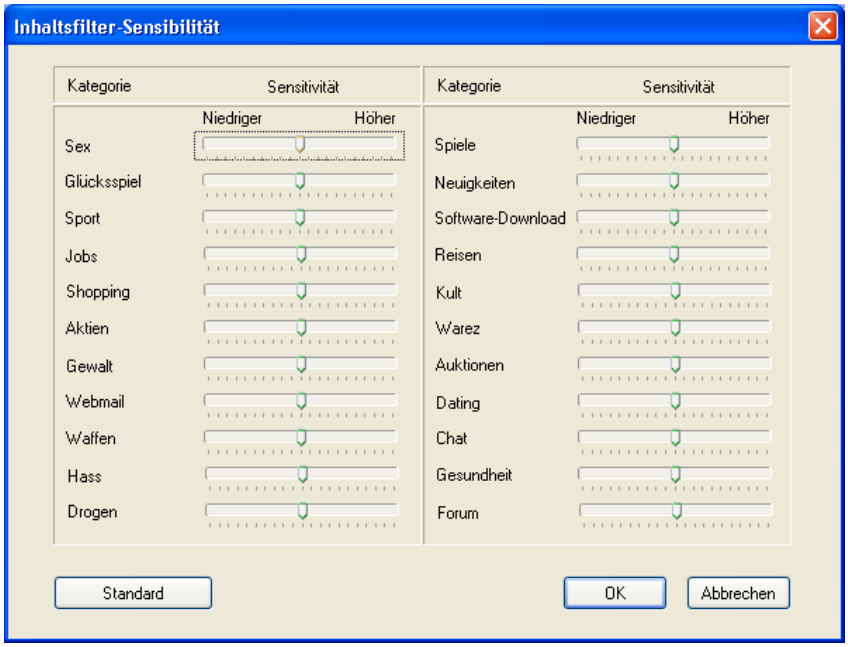
Erstellen einer Regel



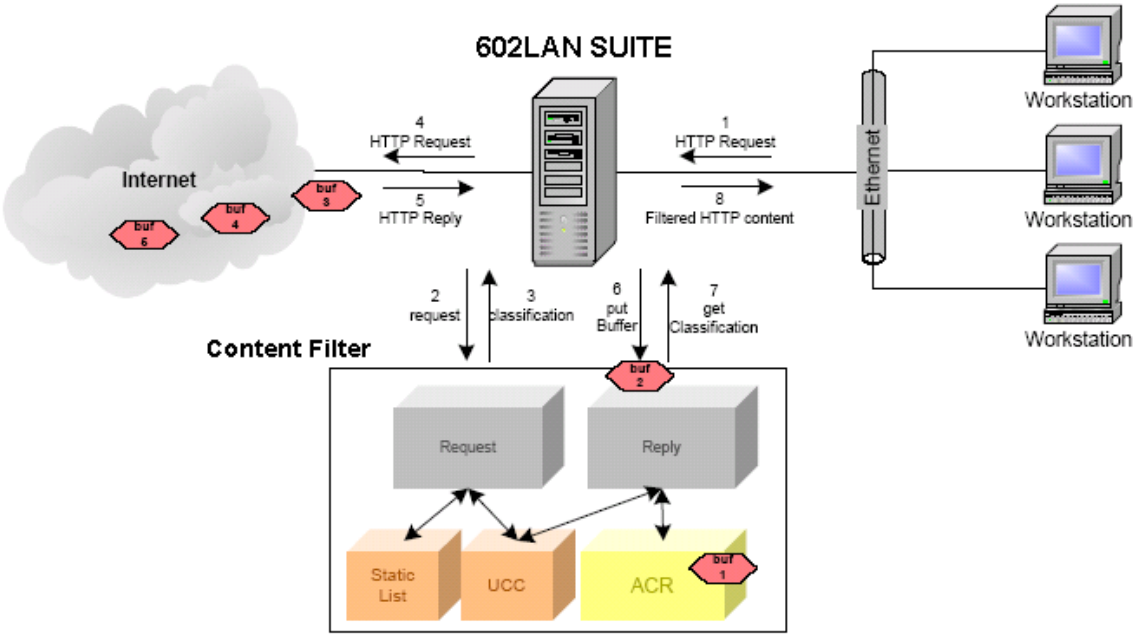
- Wählen Sie die Themen aus, die Sie beschränken wollen oder geben Sie eine URL, die Sie erlauben wollen, in die Positivliste ein oder eine, die Sie verbieten wollen, in die Negativliste.
- Geben Sie den Benutzer / Host ein, der beschränkt werden soll.
    - Für Benutzer - die Proxy-Authentifizierung muss aktiviert sein. Diese Methode ist sicherer als die Nutzung von Hosts (IP-Adressen) und wird daher empfohlen.
    - Für Hosts – hier können Sie wählen zwischen jeder Adresse / einzelnen Adressen / Subnetz / IP-Bereich. Sie müssen jedoch bedenken, dass ein Benutzer die Regel umgehen kann, indem der seine IP-Adresse ändert.
- Zeitplan – wählen Sie den Zeitbereich, in dem die Regel gelten soll.
- Bei der Erstellung eines Inhaltsfilters oder eine Negativlistenregel müssen Sie die Aktion wählen, die im Fall des Zutreffens der Regel ausgeführt werden soll:
    - Zugang blockieren und Fehlerseite anzeigen
    - Zugang blockieren und leere Seite anzeigen (weder Grafiken noch Text)
    - Zu URL umlenken – der Benutzer kann zu einer Webseite mit einer Information umgeleitet werden, z.B. zur Website Ihrer Firma.
    - Zugang protokollieren – keine andere Aktion, die Benutzeraktivitäten werden aber protokolliert. **Hinweis**: Die WWW/Proxy-Protokollierung muss aktiviert sein (im Log-Register).

Inhaltsfilter-Sensitivität

Sie können den Inhaltsfilter so einstellen, dass er Ihren Erfordernissen entspricht. Je höher die Sensitivität, desto mehr Webseiten werden klassifiziert (mit höherem Risiko für falsch-positive Bewertungen).



Arbeitsweise des 602LAN SUITE Content Filter



Wenn ein Benutzer eine Webseite im Internetbrowser anfordert, erreicht diese zuerst den Proxyserver der 602LAN SUITE. Hier wird die Anfrage zuerst mit der statischen Inhaltsliste (STL) verglichen. Wenn die Seite nicht gefunden wird, wird die Anfrage an den Klassifizierungscache (UCC) - die dynamische Inhaltsfilter-Datenbank, weitergeleitet. Wenn auch hier kein Eintrag gefunden wird, wird die Anfrage an den ACR, die künstliche Inhaltserkennung bei PureSight geschickt. Dort wird die Seite einer umfangreichen Parameteranalyse unterworfen. Nur wenn alle drei Prüfmethoden keinen Hinweis auf schädliche oder verletzende Inhalte liefern, wird die Seite an den Benutzer ausgeliefert. In allen anderen Fällen wird der Zugriff auf die Seite verweigert.

Erweiterte Zugriffskontrolle

NAT

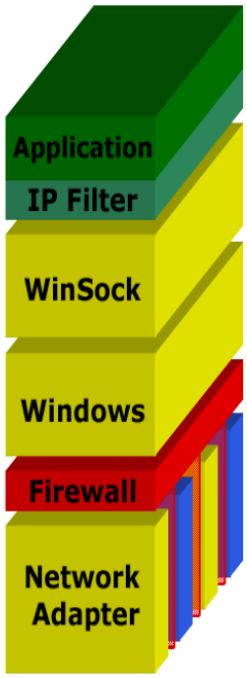
NAT (Network Address Translation) ist die Übersetzung einer IP-Adresse (Internet-Protokoll-Adresse), die in einem Netzwerk (Ihrem privaten Netzwerk) verwendet wird, zu einer anderen IP-Adresse, die in anderen Netzwerken (dem Internet) bekannt wird. NAT wandelt lokale Netzwerkadressen in eine oder mehr globale IP-Adressen und wandelt die globalen IP-Adressen von ankommenden Pakten wieder in die lokalen IP-Adressen. So wird eine gewisse Sicherheit geboten, da jede abgehende oder ankommende Anfrage durch einen Übersetzungsprozess läuft, der auch die Möglichkeit bietet die Anfrage zu qualifizieren, zu authentifizieren oder mit einer vorhergehenden Anfrage zu vergleichen. NAT behält außerdem die Anzahl der benötigten IP-Adressen und erlaubt es, mit einer einzigen IP-Adresse mit dem Internet zu kommunizieren.

Prinzip

Abgehende Pakete
Die Quell-IP-Adresse (irgendeine IP-Adresse aus Ihrem LAN) wird durch die IP-Adresse des Computers ersetzt, auf dem 602LAN SUITE eine Verbindung zum Internet hat. Pakete mit einer veränderten Quell-IP-Adresse werden an das Internet gesendet, so dass es unmöglich ist, die IP-Adresse des internen PCs zu erkennen. Jedes abgehende Paket wird in der NAT-Tabelle gespeichert, um einen unauthorisierten Zugriff über das Internet zu vermeiden.

Ankommende Pakete
Jedes vom Internet ankommende Paket, wird mit der NAT-Tabelle verglichen. Wenn das Paket dort gefunden wird, wird die Ziel-IP-Adresse zu der korrekten IP-Adresse des Computers Ihres LANs gewandelt, der ursprünglich die Internetverbindung aufgebaut hat und zu diesem geschickt. Dieser Prozess stellt die korrekte Verbindung vom Internet zu jedem Computer hinter dem NAT sicher und schützt außerdem Ihr privates Netzwerk gegen unauthorisierte Zugriffsversuche aus dem Internet.

Firewall



Die Firewall schützt den Computer, auf dem 602LAN SUITE läuft sowie das gesamte lokale Netzwerk vor unautorisierten TCP/IP-Verbindungen. Sie müssen zumindest zwei Netzwerk-Schnittstellen verwenden: 1- interne Verbindung zu Ihrem lokalen Netzwerk, 2 - externe Verbindung ins Internet. Die Firewall ist für folgende Betriebssysteme verfügbar:

- Windows 2000 Professional
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows XP Home
- Windows XP Professional
- Windows Server 20003

Zuerst muss die Sicherheitsstufe der Firewall gesetzt werden. Wählen Sie eine der folgenden Optionen:

- Hoch
- Mittel
- Niedrig
- Angepasst

HINWEIS: Ungeeignete Firewall-Einstellungen können die 602LAN SUITE-Dienste wie SMTP, POP3, Proxy, WWW usw. stören. Bitte lesen Sie dieses Kapitel aufmerksam durch!

WARNUNG: Die Firewall kommt vor dem IP-Filter. Wenn die Firewall den Zugriff auf einen bestimmten Dienst verweigert, wird diese Anforderung niemals den IP-Filter erreichen!

Wenn Sie keine Schnittstelle als interne Schnittstelle wählen, wird nur der Computer auf dem 602LAN SUITE läuft geschützt. Bedenken Sie, dass jeder Regelsatz oder jede Regel bedeutet Zugriffe zu erlauben. **Wenn keine Regeln definiert sind, wird jegliche IP-Kommunikation verweigert!**

Wählen Sie die Schnittstelle, an die Ihr lokales Netzwerk angeschlossen ist (Ihre interne Netzwerk-Schnittstelle), damit die Firewall funktioniert. Schnittstellen, die nicht ausgewählt sind, werden als externe Schnittstellen (zum Internet) angesehen.

Um Firewall-Regeln zu erstellen, ist es erforderlich, die grundlegende Funktionsweise von TCP/IP-Verbindungen zu verstehen. Hier sind die wichtigsten Prinzipien:

Aufbau von IP-Verbindungen und Zugriffsbeschränkung

Der Client-Computer (Quell-IP-Adresse:Port) baut eine TCP/IP-Verbindung zum Ziel-Computer (Server - Ziel-IP-Adresse:Port) auf.

Allgemeine Internetdienste haben immer denselben Port. Sie müssen nicht wissen, auf welchem Port der Ziel-Computer Mails zum Versenden annimmt, da jeder Server dafür den Port 25 verwendet. Wenn auf einem Computer ein Mail-Server läuft, der bereit ist, Mail anzunehmen, lauscht der Server auf Port 25 auf eingehende Mails. Ein paar allgemeine Dienste sind:

- SMTP - Port 25
- WWW - Port 80
- POP3 - Port 110
- LDAP - Port 389
- SSL (http über SSL) - Port 443

Um eine komplette Liste einzusehen, besuchen Sie: http://www.iana.org/assignments/port-numbers
Ports 0 bis 1023 sind für allgemeine Dienste reserviert und bekannt als **Gut bekannte Ports (Well Known Ports)** (z.B. FTP-Port 21). Ports von 1024 bis 49151 sind als **Registrierte Ports (Registered Ports)** bekannt (z.B. IRC Port 6667). **Dynamische/Private Ports (Dynamic/Private Ports)** sind von 49152 bis 65535.

Sie denken vielleicht, dass die Anwendung, die Mails versendet, dafür den Port 25 verwendet, doch das ist nicht der Fall. Die Anwendung fordert stattdessen gewöhnlicherweise vom Betriebssystem einen Socket (Voraussetzung, um eine TCP/IP-Verbindung aufzunehmen) an, d.h. es fragt nach einem Port und bekommt einen solchen zugeteilt. Jeder bislang unbenutzte Port kann verwendet werden (die Anwendung muss nicht einmal wissen, was die exakte Port-Nummer ist), doch das Betriebssystem wird einen Port mit einer Nummer oberhalb 1023 verwenden. Dieser Port wird nur so lange wie erforderlich verwendet und dann wieder freigegeben. Jedes TCP/IP-Paket enthält Informationen über die Quell-IP-Adresse und den Quell-Port, sowie die Ziel-IP-Adresse und den Ziel-Port. Der von der Anwendung angeforderte Port oberhalb 1023 ist der Quell-Port, der Standard-Port für den Dienst ist der Ziel-Port. Dies hört sich kompliziert an, doch das zugrunde liegende Prinzip ist einfach zu verstehen: wenn ein Programm einen Port oberhalb 1023 nutzt, kommen Antworten auch an diesen Port und können so der entsprechenden Anwendung zugeordnet werden. Etwas komplizierter wird es noch: Da die Standard-Ports für einen Dienst für alle Clients sind, verwendet der Server diesen nicht für die eigentliche Datenübertragung. Der Server lauscht nur auf diesem Port. Sobald eine Verbindung aufgebaut wird, reicht es die Verbindung an einen lokalen Port oberhalb 1023 auf dem Server weiter, und lauscht sofort wieder auf dem Standard-Port für weitere Verbindungen. So kann ein Webserver zu mehreren tausend Clients Verbindungen aufbauen.

Protokolle
TCP (Transport Control Protocol) ist als verbindungsorientiertes Protokoll bekannt. Das bedeutet, dass eine Verbindung aufgebaut und aufrecht erhalten wird, bis alle Nachrichten der Kommunikationspartner ausgetauscht sind. TCP ist verantwortlich jede Nachricht in einzelne Pakete aufzuteilen, die vom IP-Protokoll gehandhabt werden, und auf dem Ziel-Computer aus diesen einzelnen IP-Paketen dann wieder eine komplette Nachricht zusammenzusetzen.

UDP-Pakete (User Datagram Protocol) bauen keine "permanente" Verbindung auf. Der Absender sendet UDP-Pakete und kümmert sich dann nicht weiter um sie. Um diese Art von Verbindungen zu handhaben, ist es erforderlich, die erlaubte Richtung der UDP-Verbindung zu setzen, um Verbindungen vom Ihrem lokalen Netzwerk zum Internet und Antworten aus dem Internet anzunehmen. Beispiel: Ein Computer vom Ihrem lokalen Netzwerk sendet eine DNS-Anforderung an einen DNS-Server im Internet und erwartet eine Antwort. Diese Antwort ist ein Antwort-Paket.

Das ICMP-Protokoll ist ein Dienstprotokoll. Es signalisiert in IP-Netzwerken verschiedene Ereignisse: Ziel nicht erreichbar (Destination Unreachable), Weiterleitung (Redirect), Echo-Anforderung (Echo Request), Router-Bewerbung (Router Advertisement), Router-Antwort (Router-Solicitation). Das ICMP-Protokoll wird von den Befehlen PING und TRACERT verwendet. "Destination Unreachable" und "Redirect"-Nachrichten werden als die gefährlichsten angesehen. Wenn Sie grundlegende Netzwerk-Diagnostik erlauben möchten, können Sie die folgenden Nachrichten erlauben:

- Ausgehende ICMP-8-Nachrichten (Echo-Anforderung)
- Ankommende ICMP-0-Nachrichten (Echo-Antwort - wird vom PING-Befehl verwendet)
- Ankommende ICMP-11-Nachrichten (Zeitüberschreitung - wird vom TRACERT-Befehl verwendet)

Wir empfehlen, andere ICMP-Nachrichten zu sperren.

Firewall-Einstellungen

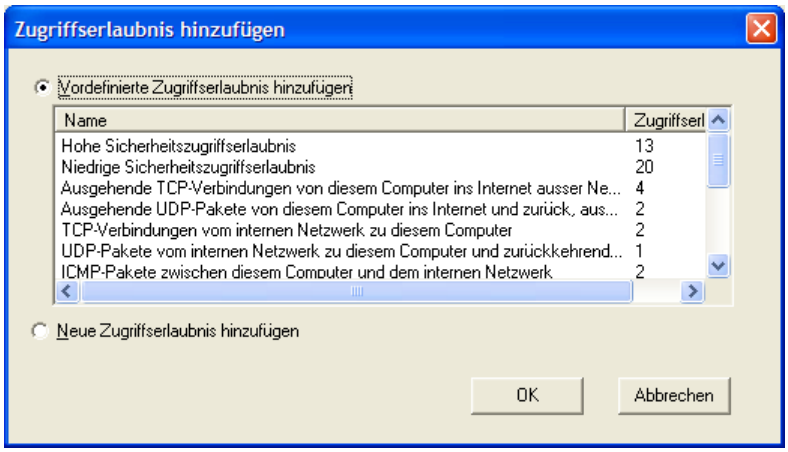
Der Computer auf dem 602LAN SUITE läuft, muss mindestens **zwei Netzwerk-Schnittstellen haben:**

- **Intern** - Netzwerk-Karte, die mit Ihrem lokalen Netzwerk (LAN) verbunden ist.
- **Extern** - Analogmodem, ISDN-Adapter oder zweite Netzwerk-Karte für die Verbindung mit dem Internet.

Um die Firewall zu verwenden, aktivieren Sie zunächst die Option "Firewall" in der linken oberen Ecke des Registers "Firewall". Dann wählen Sie Ihre interne(n) Netzwerk-Schnittstelle(n). Die Firewall schützt den Computer, auf dem 602LAN SUITE läuft, sowie das an die interne Netzwerk-Schnittstelle angeschlossene lokale Netzwerk, indem sie TCP/IP-Pakete filtert.
Nun können Sie die Sicherheitsstufe wählen. Wir empfehlen, eine der vordefinierten Sicherheitsstufen auszuwählen: "Hoch", "Mittel" oder "Niedrig". Lesen Sie die Beschreibung auf der rechten Seite, wenn Sie eine Sicherheitsstufe auswählen.

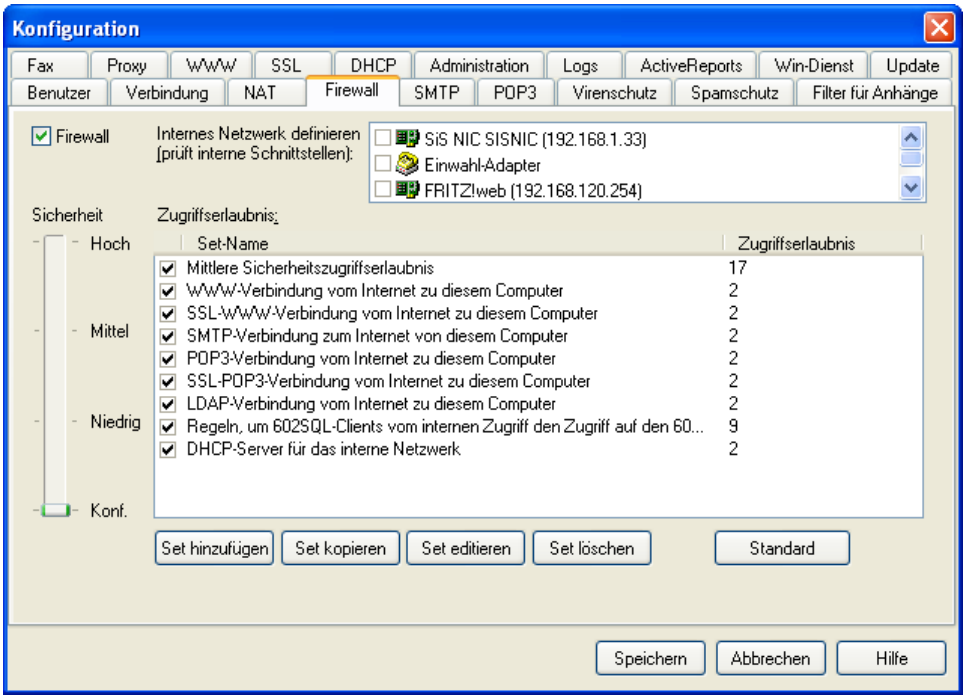
SMTP/POP3/WWW/LDAP-Server mit der hohen oder mittleren Sicherheitsstufe verwenden

Sobald Sie die Sicherheitsstufe auf "Hoch" oder "Mittel" setzen, werden alle TCP-Verbindungen vom Internet abgelehnt, inkl. eventueller Anforderungen an die SMTP-, WWW-, SSL-WWW, POP3-, SSL-POP3- und LDAP-Server von 602LAN SUITE. Sie können den Zugriff auf einfache Weise erlauben, indem Sie den geeigneten vordefinierten Regelsatz hinzufügen.


Zugriffserlaubnis hinzufügen
Vordefinierte Zugriffserlaubnis hinzufügen:
Name
Zugriffserl
Hohe Sicherheitszugriffserlaubnis 13
Niedrige Sicherheitszugriffserlaubnis 20
Ausgehende TCP-Verbindungen von diesem Computer ins Internet ausser Ne... 4
Ausgehende UDP-Pakete von diesem Computer ins Internet und zurück, aus... 2
TCP-Verbindungen vom internen Netzwerk zu diesem Computer 2
UDP-Pakete vom internen Netzwerk zu diesem Computer und zurückkehrend... 1
ICMP-Pakete zwischen diesem Computer und dem internen Netzwerk 2
Neue Zugriffserlaubnis hinzufügen
OK
Abbrechen

Angepasste Sicherheitsstufe

Wenn Sie "Angepasst" als Sicherheitsstufe wählen, können Sie alle Firewall-Einstellungen selbst kontrollieren. Sie können vordefinierte Regelsätze hinzufügen, neue erstellen, Regelsätze bearbeiten oder löschen.



Einen neuen Regelsatz hinzufügen

Klicken Sie auf "Set hinzufügen", um einen neuen Regelsatz hinzuzufügen. Das Fenster "Zugriffserlaubnis hinzufügen" erscheint. Hier können Sie zwischen zwei Optionen wählen:

- **Vordefinierte Zugriffserlaubnis hinzufügen** - Hier finden Sie alle vordefnierten Regelsätze. Sie finden hier ebenfalls die Regelsätze für die hohe, mittlere und niedrige Sicherheitsstufe. Diese können Sie ändern, wenn Sie sie unter einem anderen Namen speichern.
- **Neue Zugriffserlaubnis hinzufügen** - Wählen Sie diese Option, um einen neuen Regelsatz hinzuzufügen.

Einen neuen Regelsatz hinzufügen

Klicken Sie auf "Neue Zugriffserlaubnis hinzufügen" und dann auf "OK". Geben Sie den Namen des Regelsatzes in "Zugriffsrechtname" ein und klicken Sie auf "Hinzu". Das Fenster "Paket-Zugriffserlaubnis" erscheint.

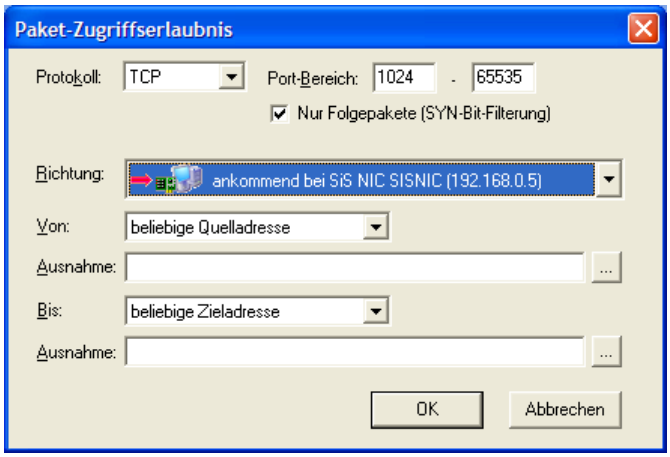
Wählen Sie das IP-Protokoll:

- **Alle** - Alle Protokolle der IP-Protokoll-Familie werden gefiltert
- **TCP** - Geben Sie den Portbereich an. Wenn Sie die Option "Nur Folgepakete" aktivieren, wird die Firewall alle TCP-Pakete verwerfen, deren SYN-Flag gesetzt ist. Dieses wird beim ersten TCP-Paket, das eine Verbindung aufbaut, gesetzt. Die Firewall verbietet dann also den Aufbau einer neuen Verbindung für den Portbereich und die Richtung.
- **UDP** - Geben Sie den Portbereich ein. Wählen Sie bei Bedarf "Antwortpakete auch erlauben".
- **ICMP** - Wählen Sie die Nachrichten, die Sie erlauben möchten. Empfohlen: "Echo (Outgoing Echo Request)", "Echo-Antwort (Incoming Echo reply)" und "Zeit überschritten (Time exceeded)".
- **Anderes** - Die Firewall kann jegliches IP-Protokoll filtern. Geben Sie die Nummer des Protokolls an, das sie filtern möchten.

Bestimmte IP-Adressen ausschließen

Obwohl alle Regeln für die Firewall Zugriffe erlauben, hat die Firewall die Fähigkeit, IP-Adressen von einem bestimmten Netzwerk-Adapter auszuschließen. Beispiel: Jemand aus dem Internet versucht andauernd eine Verbindung zu Ihrem SMTP-Server auf Port 25 aufzubauen. Sie können diese Anfragen ausschließen:

1. Wählen Sie die Regel "SMTP-Verbindung zum Internet von diesem Computer" und klicken Sie auf "Set editieren".
2. Klicken Sie auf die TCP (Port 25)-Regel und dann auf "Bearbeiten".
3. Als Richtung wählen Sie "ankommend bei x", wobei "x" für den entsprechenden Netzwerk-Adapter steht.
4. Von:/Bis: sollte auf "beliebige Quelladresse" gestellt sein.
5. In dem ersten "Ausnahme"-Feld geben Sie die IP-Adresse des Angreifers an. Sie können eine IP-Adresse (192.168.1.1), mehrere mit Kommas hintereinander, einen Bereich von IP-Adressen (192.168.1.1-192.168.1.20) oder ein IP-Subnetz (192.168.1.0/255.255.255.0) angeben.
6. Klicken Sie auf "OK", benennen Sie den Namen des Zugriffsrechtes um, indem Sie z.B. die Nummer 2 am Ende des Namens hinzufügen, klicken Sie noch einmal auf "OK" und dann auf "Speichern". Nun wird jeder Computer Mails an Ihren SMTP-Server ausliefern können mit Ausnahme des angreifenden Computers.



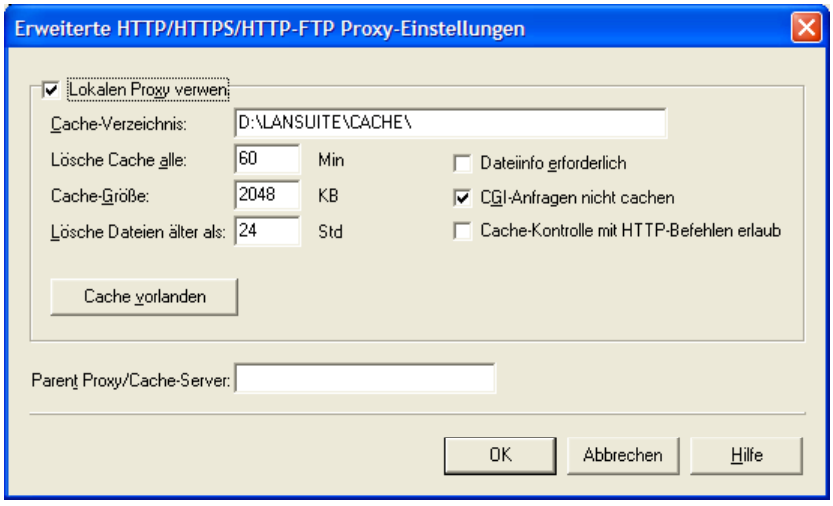
Proxy-Cache

Das Register "Proxy" enthält vier weitere Register. "Proxy-Server" dient der Proxy-Server-Konfiguration, "Site-Zugriff", "Weitergeleitete Links" und "IP-Filter" betreffen die Sicherheit der Proxy-Server.

Den lokalen Proxy-Cache verwenden - Register "Proxy-Server"

Die Option "Lokalen Proxy verwenden" ist empfehlenswert für langsame Verbindungen, bei denen die Bandbreite eine große Rolle spielt. Wenn Sie diese Option einschalten, aktivieren Sie den Proxy-Cache, der angeforderte Webseiten auf dem 602LAN SUITE-Server speichert, damit diese bei erneutem Abruf direkt von der Festplatte geliefert werden und nicht mehr aus dem Internet geladen werden müssen. Sie finden die Option im Register "Proxy", wenn Sie auf "Erweiterte HTTP-Proxy-Einstellungen" klicken. Für schnelle Verbindungen wie DSL/Kabel/T1 bietet diese Funktion wenig Vorteile. Die folgenden Optionen erlauben die Anpassung des Proxy-Cache an Ihre Wünsche:

- **Datei-Info erforderlich** – Die meisten Webserver senden Informationen über eine Datei, die 602LAN SUITE helfen, zu entscheiden, ob diese vollständig übertragen wurde. Ist diese Option aktiviert, werden nur vollständig geladene Dateien im Cache gespeichert.
- **CGI-Anfragen nicht cachen** – 602LAN SUITE wird die Ergebnisse von CGI-Anfragen nicht zwischenspeichern.
- **Cache-Kontrolle mit HTTP-Befehlen erlauben** – 602LAN SUITE befolgt HTTP-Cache-Befehle (Beispiel: Pragma: no-cache)



Cache vorladen

Wenn Client-Computer in Ihrem lokalen Netzwerk oft große Dateien aus dem Internet laden, können Sie diese Dateien auch von einem lokalen Datenträger laden (z.B. CD-ROM oder Festplatte). Clients müssen Dateien nicht von der Internet-Webseite sondern nur vom 602LAN SUITE-Server laden.

Geben Sie in das Feld "Dateien von URL laden" die Internet-URL an, wo die angeforderten Dateien ursprünglich gespeichert sind. Unter "Von Pfad laden" geben Sie dann den vollen Pfad zu dem Verzeichnis an, wo Sie die Dateien für die betreffende URL gespeichert haben. Alle vorab geladenen Dateien müssen in der gleichen Verzeichnisstruktur vorliegen wie auf der Webseite im Internet. Wenn ein Client (z.B. ein Webbrowser) von Ihrem lokalen Netzwerk aus ein Dokument aus dem Internet anfordert, prüft der Proxy-Server zunächst, ob im Internet eine neuere Version als auf dem lokalen Datenträger. Wenn 602LAN SUITE diese Prüfung nicht jedes Mal vornehmen soll, aktivieren Sie "Nicht nach neueren Versionen der Dateien suchen für mindestens x Tage" und geben Sie die Anzahl der Tage an.

Übergeordneter Proxy-/Cache-Server

Wenn Ihr Netzwerk einen dem 602LAN SUITE-Server übergeordneten Proxy-Server verwenden, können Sie diesen wie folgt angeben:

1. Aktivieren Sie das Register "Proxy" und klicken Sie auf "Erweiterte HTTP-Proxy-Einstellungen".
2. Geben Sie die IP-Adresse des übergeordneten Proxy- oder Cache-Server, den Sie verwenden möchten, in das Feld "Übergeordneter Proxy-/Cache-Server" ein.

Site-Zugriffskontrolle

Benutzer, deren Zugriffe zugelassen oder abgewiesen werden sollen, werden durch Ihre IP-Adresse und IP-Maske angegeben. Sie können bestimmte URLs für einen einzelnen Computer oder ein Teilnetzwerk freigeben oder sperren. Um das gesamte Netzwerk anzugeben, geben Sie 0.0.0.0 als Quell-IP-Adresse und Quell-IP-Maske ein. Wenn nur ein bestimmter Computer oder eine Gruppe von Computer betroffen sein soll, geben Sie die IP (z.B. 192.168.1.23 mit Maske 255.255.255.255) oder Gruppe (z.B. 192.168.1.0, Maske 255.255.255.0) ein. Anders als beim IP-Filter werden die freigegebenen oder gesperrten Orte (Sites) durch ihren Namen, ihre URL oder einen Teil davon definiert. "*" und "?" können als Platzhalter verwendet werden (DOS-Konvention: "*" = alles, mehrere Zeichen, "?" = Maske, ein Zeichen).

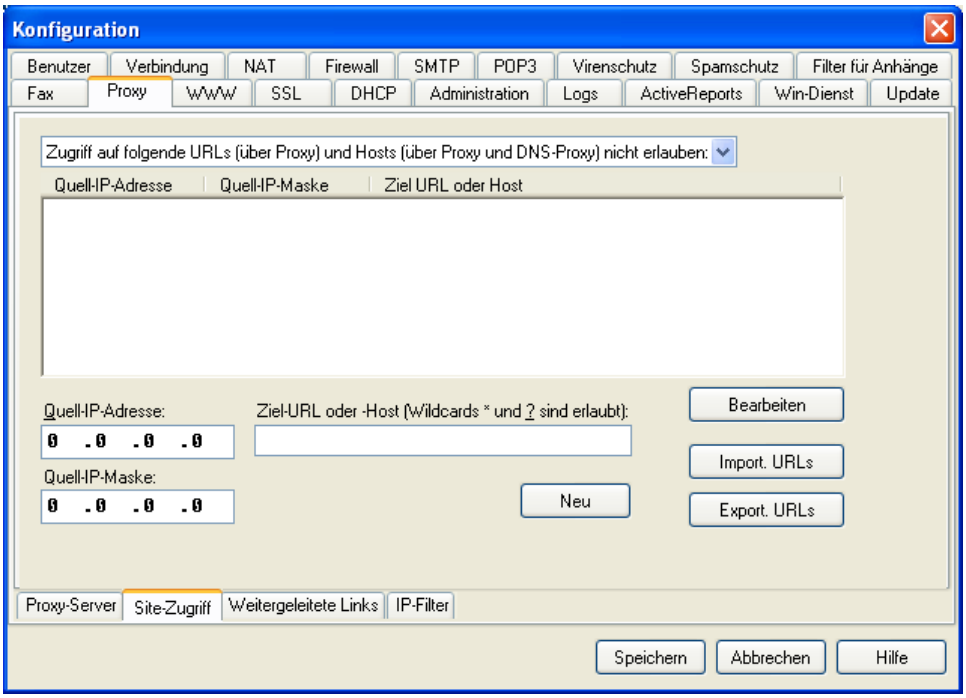
Nutzen Sie die Eingabefelder und die Schaltfläche "Hinzu", um die Namen für freigegebene oder gesperrte URLs anzugeben. Sie können die Platzhalter "*" und "?" verwenden. Geben Sie die IP-Adresse und die Maske des betreffenden Computers oder Netzwerks an.

Beispiele:

"*.werbung*.*" sperrt den Zugriff auf Server, deren Name mit "werbung" beginnt, für alle Dienste (HTTP, HTTPS, FTP). *.einkaufen.?? sperrt den Zugriff auf die Domain "einkaufen" für alle zweiteiligen Domänen-Namen (Subdomänen) und alle Dienste. "www.kein-zugriff.de" sperrt den Zugriff auf den Server mit diesem Namen.

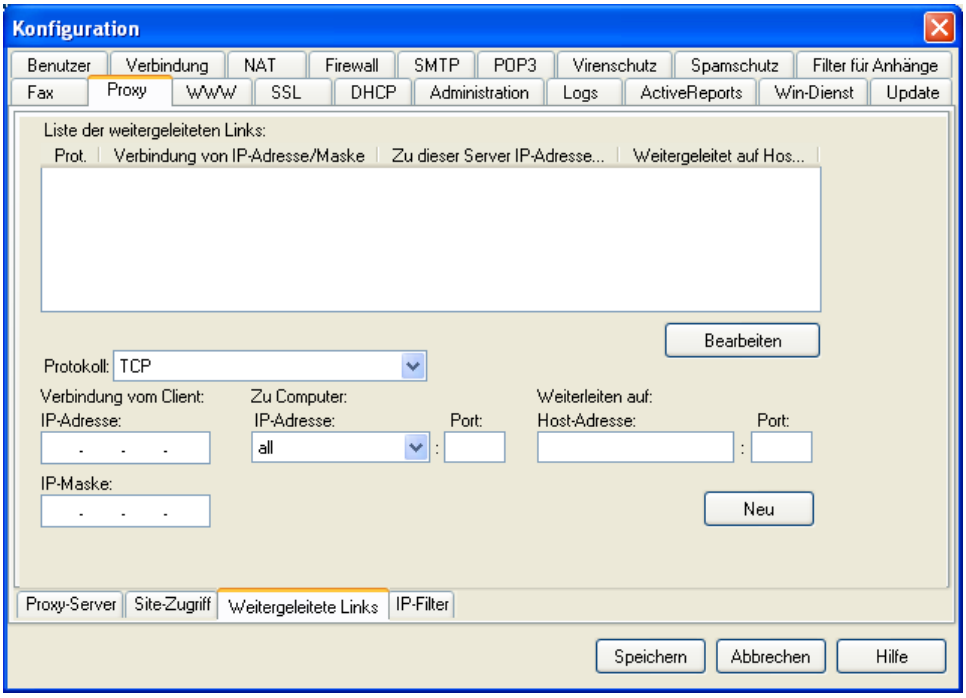
Sie können die Schaltfläche "Löschen/Bearbeiten" verwenden, um eine bereits bestehende Regel zu löschen oder zu bearbeiten. Wenn Sie eine Regel bearbeiten, klicken Sie wieder auf "Hinzu", wenn Sie fertig sind.

URLs können in eine Datei exportiert oder von einer Datei importiert werden. Das Format der Datei ist einfacher Text mit einer URL pro Zeile.



Weitergeleitete Links

Weitergeleitete Links dienen als alternative Methode, um einem lokalen Computer Zugriff auf das Internet zu ermöglichen. Es ist geeignet für Anwendungen, die weder SOCKS noch PROXY unterstützten, und verbindet nur mit einem Computer auf dem Internet (z.B. eine Verbindung zu einem NTTP NEWS-Server, VNC, POP3, usw.). Es ist möglich für weitergeleitete Links mit dem TCP- oder dem UDP-Protokoll zu verwenden.



Funktionsweise

Das Anwendungsprogramm auf dem Computer im lokalen Netzwerk möchte eine TCP/IP-Verbindung mit einem bestimmten Computer im Internet aufbauen. Anstatt die Adresse des betreffenden Computers einzugeben, wird die Adresse des 602LAN SUITE-Servers angegeben. Im Register "Weitergeleitete Links" geben Sie dann an, dass wenn der betreffende Computer den Server auf einem bestimmten Port kontaktiert, alle seine Zugriffe an einen bestimmten Computer im Internet weitergeleitet werden sollen. Dies erstellt über den 602LAN SUITE-Server einen virtuellen Link zwischen zwei Computern. Die Verbindung zwischen zwei Computern wird durch den 602LAN SUITE-Server vermittelt und weitergeleitet.

Vorteile:

Der Client muss weder Proxy- noch Firewall-Zugriff unterstützen.

Nachteile:

- Jede Verbindung benötigt einen eigenen weitergeleiteten Link.
- Jeder weitergeleitete Link muss einen anderen Port verwenden.

Einstellungen

Setzen Sie diese Einstellungen im Register "Weitergeleitete Links":

- **Protokoll:** Wählen Sie für jeden weitergeleiteten Link das Protokoll (TCP oder UDP, UDP1, UDP2). Zu den UDP-Protokoll-Einstellungen siehe weiter unten.
- **Verbindung vom Client** – Geben Sie die IP-Adresse und die IP-Maske für den lokalen Computer an, der den weitergeleiteten Link verwenden soll. Nur die angegebenen Computer dürfen die Verbindung aufnehmen.
- **IP-Adresse:** Geben Sie die IP-Adresse des Computers an, der auf diesen Link zugreifen dürfen soll. Sie können auch ein Teilnetzwerk mit mehreren Computern angeben. Beispiel: Wenn Sie jedem Computer in Ihrem lokalen Netzwerk den Zugriff erlauben wollen, geben Sie Ihre Netzwerk-Adresse an. Diese erhalten Sie, wenn Sie die IP-Adresse des 602LAN SUITE-Server nehmen und die letzte Zahl durch eine "0" ersetzen (z.B. 192.168.1.0). Um nur einen Computer den Zugriff zu erlauben, geben Sie dessen IP-Adresse an. Um jedem Computer den Zugriff zu erlauben, geben Sie 0.0.0.0 an.

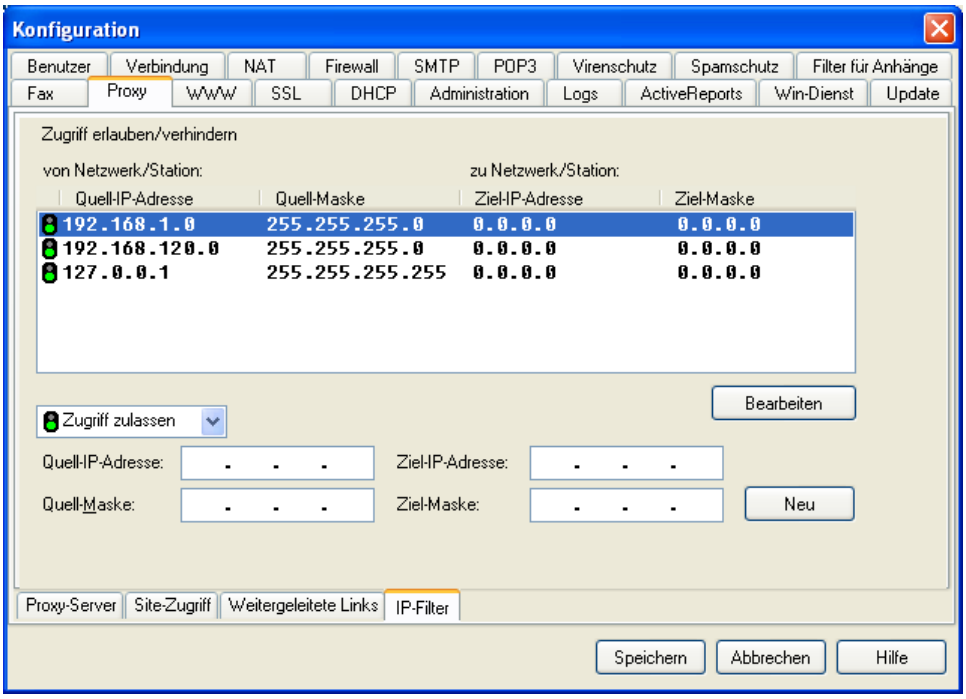
- **IP-Maske:** Dies ist die Teilnetzmaske für die Computer, denen Sie den Zugriff erlauben wollen. Eine detaillierte Erklärung wie Teilnetzmasken funktionieren, führt zu weit. Einige Beispiele: Wenn Sie nur einem Computer den Zugriff erlauben möchten, geben Sie 255.255.255.255 ein. Wenn Sie einem Netzwerk den Zugriff erlauben möchten, geben Sie 255.255.255.0 ein. Wenn Sie jedem Computer dem Zugriff erlauben möchten, geben Sie 0.0.0.0 ein.
- **Zu Computer** – Dies gibt die Netzwerk-Schnittstelle an, die Sie zugänglich machen möchten.
- **IP-Adresse**: Alle Schnittstellen. Sie können dies ändern, wenn Sie die Sicherheit des weitergeleiteten Links erhöhen möchten.
- **Port**: Dies ist der Port, den der Server für den weitergeleiteten Link verwendet. Sie können keinen Port verwendet, der bereits anderswo benutzt wird. Wenn Sie bereits einen weitergeleiteten Link auf Port 9000 haben, können Sie keinen weiteren Link mit diesem Port verwenden. Die Ports 80, 21, 23 sind bereits belegt, ebenso wie der Port 1080, wenn Sie einen Proxy-Server verwenden. Je nach Ihrer Konfiguration sind weitere Ports bereits belegt. Der weitergeleitete Link funktioniert nicht, wenn der betreffende Port bereits verwendet wird.
- **Weiterleiten auf:** Geben Sie die Host-Adresse und den Port des Computers im Internet an, zu dem der Client im lokalen Netzwerk eine Verbindung aufbauen können soll.
- **Host-Adresse**: Geben Sie den Domänen-Namen oder die IP-Adresse des Computers an, den Sie kontaktieren wollen. Wenn Sie einen Mail-Server kontaktieren wollen, geben Sie dessen Domänen-Namen ein (z.B. "pop.ihr-server.de").
- **Port**: Das ist der Port, auf dem der Computer im Internet auf Verbindungen wartet. Diesen Port können Sie für mehrere weitergeleitete Links verwenden.

Klicken Sie auf "Hinzu", sodass Ihr Eintrag übernommen wird. Wenn Sie fertig sind, klicken Sie auf "Speichern", um die Konfiguration zu speichern.

WARNUNG: Sie können nicht zwei Dienste mit dem gleichen Port auf der gleichen Netzwerk-Schnittstelle verwenden.

Proxy-IP-Filter-Konfiguration

Der IP-Filter definiert, welche Verbindungen über den Proxy- und den SOCKS-Dienst zugelassen werden. Mit Hilfe des IP-Filters definieren Sie, welche Verbindungen über den SOCKS- oder Proxy-Server aufgenommen werden können. Sie erstellen eine Liste von Netzwerken und Computern und definieren, ob der Zugriff zu ihnen freigegeben oder gesperrt wird. Die IP-Filterregeln werden von oben nach unten abgearbeitet. Geben Sie in die Felder "Quell-IP-Adresse" und "Quell-Maske" die IP-Adresse und die Maske des Computers oder des Netzwerks an, von wo aus die Netzwerk-Anforderung gesendet wird. Geben Sie in die Felder "Ziel-IP-Adresse" und "Ziel-Maske" ein, wohin die Anforderungen gerichtet werden. Dann geben Sie noch an, ob der Zugriffe gemäß dieser Regeln freigegeben oder gesperrt werden sollen. Rot bedeutet, der Zugriff ist gesperrt, Grün bedeutet, der Zugriff ist freigegeben.



Begriffe

Ein TCP/IP-Computernetzwerk wird durch die IP-Adresse und die Maske definiert. Die IP-Adresse definiert die adressierten Bereich von IP-Adresse oder eine einzelne IP-Adresse und die Maske gibt dazu passend die Größe des Netzwerks an (die maximale Anzahl von IP-Adressen).

Masken-Beispiele

255.255.255.255 Einzelner Computer mit der angegebenen IP-Adresse.
255.255.255.0 Alle Computer in einem Klasse-C-Netzwerk.
255.255.255.224 Ein Teilnetzwerk mit 32 IP-Adressen.
0.0.0.0 Alle IP-Adressen (inkl. Internet)

Funktionsweise des IP-Filters

Mit dem IP-Filter können Sie angeben, ob eine Verbindung zwischen zwei bestimmten Computer freigegeben oder gesperrt werden soll (z.B. wenn ein Benutzer in Ihrem lokalen Netzwerk auf www.software602.com zugreifen möchte). 602LAN SUITE trifft eine logische Entscheidung basierend auf der IP-Adresse des Computers, der eine Verbindung aufbauen möchte (Quell-IP-Adresse) und der IP-Adresse des Ziel-Computers (Ziel-IP-Adresse). Der IP-Filter folgt dieser Regel:

Um Zugriff zu gewähren, müssen die folgenden Bedingungen erfüllt sein.

QUELL-IP UND QUELL-MASKE = WER-IP UND QUELL-MASKE
ZIEL-IP UND ZIEL-MASKE = WOHIN-IP UND ZIEL-MASKE
Die Verbindung wird zugelassen, wenn das Ergebnis dieser beiden logischen Operationen "wahr" ist und die Regel auf "Zugriff zulassen" (grün) eingestellt ist.
Die IP-Filterregeln werden von oben nach unten geprüft. Sie haben folgende Möglichkeiten:

- Zugriff zulassen (grün): Nur bestimmten Benutzern Internet-Zugriff gewähren.
- Zugriff verbieten (rot): Nur bestimmten Benutzern Zugriff verbieten.

Wenn Sie eine Regel nach oben oder unten verschieben möchten, wählen Sie die Regel aus und drücken Sie Strg + Pfeil-Hoch oder Strg + Pfeil-Runter. Wenn Sie eine Regel von der Liste löschen möchten, wählen Sie die Regel aus und klicken Sie auf "Löschen". Sie können die Regel dann auch bearbeiten und dann wieder auf "Hinzu" klicken.

HINWEIS: Wenn Sie die einen übergeordneten Proxy-/Cache-Server verwenden, können Sie die Kommunikation nicht mit Hilfe der IP-Maske beschränken, da der Proxy-Server in diesem Fall die IP-Adresse des Ziel-Computers nicht überprüft. Um für bestimmte Computer den Zugriff zu sperren, verwenden Sie das Register "Site-Zugriffskontrolle".

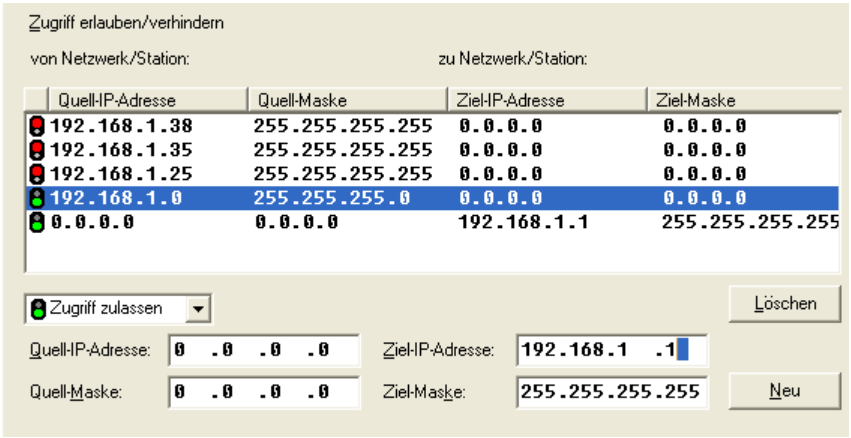
IP-Filter-Einstellungen – Beispiel 1

Sie benötigen für Ihre Firma die folgenden IP-Filter-Einstellungen:

- Für drei Computer mit den folgenden IP-Adressen den Zugriff sperren: 192.168.1.25, 192.168.1.35, 192.168.1.38
- Für alle anderen Computer Internet-Zugriff freigeben.
- Externe Benutzer müssen vom Internet aus nur auf einen Computer mit der IP-Adresse 192.168.1.1 IP-Zugriff erhalten.

Lösung:

- Die ersten drei Regeln verweigern den drei Computern mit den IP-Adressen 192.168.1.25, 192.168.1.35, 192.168.1.38 den Zugriff zu jeglichen Computern durch die Firewall hindurch. (Dies sperrt für diese drei Computer den Zugriff auf das Internet.)
- Die vierte Regel gewährt allen Computern des 192.168.1.0-Netzwerk die Kommunikation mit jedem Computer durch die Firewall hindurch. Diese Regel erlaubt allen Computern des Netzwerks, auch denen mit den IP-Adressen 192.168.1.25, 192.168.1.35 und 192.168.1.38, den Zugriff auf das Internet. Da jedoch die IP-Filterregeln von oben nach unten abgearbeitet werden, haben die Computer mit den IP-Adressen 192.168.1.25, 192.168.1.35, 192.168.1.38 keinen Internet-Zugriff.
- Die fünfte Regel gewährt jegliche Kommunikation mit dem Computer mit der IP-Adresse 192.168.1.1 durch die Firewall hindurch. Diese Regel erlaubt jedem Internet-Computer den Zugriff auf den lokalen Computer mit der IP-Adresse 192.168.1.1.



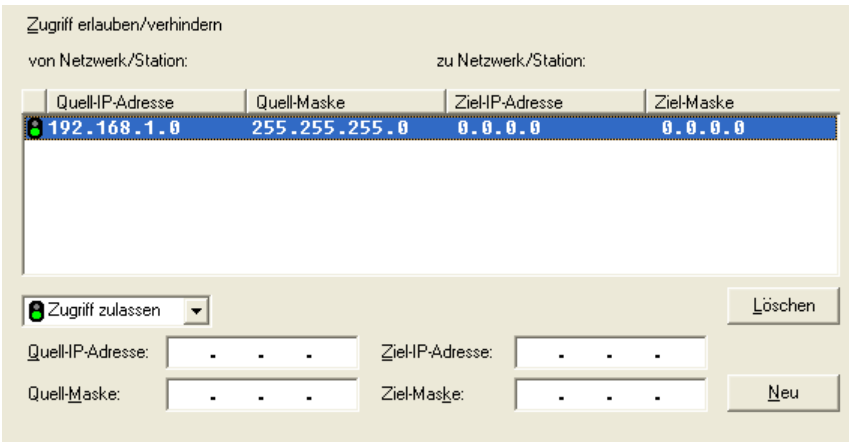
HINWEIS: Wenn die vierte Regel ganz am Anfang wäre, wäre der Zugriff auf die drei Computer mit den IP-Adressen 192.168.1.25, 192.168.1.35, 192.168.1.38 erlaubt.

IP-Filter-Einstellungen – Beispiel 2

Alle Computer des 192.168.1.0-Netzwerks können mit allen Computern im Internet kommunizieren und das lokale Netzwerk ist für alle Internet-Computer unzugänglich.

Lösung:

- Definieren Sie eine Regel für das interne Netzwerk. Die Regel unten legt fest, dass die Computer mit den IP-Adressen von 192.168.1.1 bis 192.168.1.254 auf jeglichen Ziel-Computer (0.0.0.0 für alle IP-Adressen) zugreifen können.



SSL-Konfiguration

Das SSL-Protokoll (Secure Socket Layer) arbeitet zwischen der Netzwerk-Ebenen und den Anwendungsprotokollen. Es bietet Server-Authentifikation, verschlüsselte Verbindungen und Client-Authentifikation (optional). Im Register "SSL" können Sie die SSL-Unterstützung konfigurieren sowie öffentliche und private Schlüssel erstellen. SSL funktioniert wie folgt:

- Kommunikation mittels SSL geschieht durch ein Schlüsselpaar: einen öffentlichen und einen privaten Schlüssel.
- Der private Schlüssel wird vom Server verwenden, um Daten zu verschlüsseln.
- Der öffentliche Schlüssel (Zertifikat) wird vom Client verwendet, um Daten vom Server zu entschlüsseln. Die Zertifizierungsstelle (Certification Authority - CA) überprüft die Identität des Zertifikatseigners, so dass der Client sicher sein kann, mit dem korrekten Server verbunden zu sein. Am einfachsten ist es, ein selbst signiertes Zertifikat zu verwenden (der Server arbeitet als Zertifizierungsstelle).

Eine SSL-Sitzung läuft wie folgt ab:

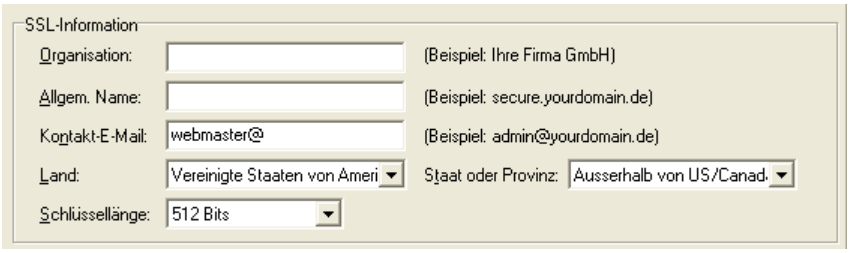
- SSL-Server-Authenfikation erlaubt es einem Benutzer, die Identität des Servers nachzuprüfen.
- Eine verschlüsselte SSL-Verbindung erfordert, dass jegliche Kommunikation zwischen Server und Client vom Absender verschlüsselt und vom Empfänger entschlüsselt wird.
- SSL-Client-Authentifikation erlaubt dem Server, die Identität eines Benutzers (Client) zu bestätigen.
- Client und Server kommunizieren beim SSL-Protokoll wie folgt (Handshake):
    - Der Server authentifiziert sich gegenüber dem Client.
    - Server und Client teilen sich mit, welche kryptografischen Algorithmen (Ciphers) Sie unterstützen.
    - Der Client authentifiziert sich gegenüber dem Server (optional).
    - Es werden auf öffentlichen Schlüsseln basierende Verschlüsselungstechnologien verwendet.
    - Es wird eine verschlüsselte SSL-Verbindung aufgebaut.

Das Register "SSL" ist in zwei Register mit Optionen für SSL für die SSL-SMTP-, SSL-POP3- und SSL-WWW-Server unterteilt.

Allgemein

Um sichere Kommunikation zwischen den SMTP-, POP3- oder WWW-Servern und ihren Clients verwenden möchten, müssen Sie zunächst den öffentlichen und den privaten Schlüssel erstellen. Geben Sie unter "SSL-Information" Ihre Informationen für das Erstellen des Schlüsselpaars ein:

- **Organisation** – Name der Organisation
- **Allgemeiner Name** – Der Domänen-Name oder die IP-Adresse des Computers, auf dem 602LAN SUITE läuft.
- **Kontakt-Mail** – Die Mail-Adresse des Administrators oder Webmasters.
- **Land** – Wählen Sie Ihr Land.
- **Staat oder Provinz** – Wählen Sie ihren Staat oder Provinz. Für Deutschland "Außerhalb der USA oder Canada".
- **Schlüssellänge** – Wählen Sie die Schlüssellänge. Ein längerer Schlüssel erhöht die Sicherheit, jedoch auch die übertragene Datenmenge.



Nun haben Sie zwei Möglichkeiten: Erstellen Sie ein selbst signiertes Zertifikat oder lassen Sie Ihren öffentlichen Schlüssel von einer Zertifizierungsstelle (Certification Authority - CA) signieren.

- **Selbst signiert:** Ein selbst signierter Schlüssel ist kostenlos, wird jedoch nicht automatisch von Webbrowser erkannt und als vertrauenswürdig eingestuft. Der Webbrowser wird eine Warnung anzeigen, wenn er auf einen SSL-WWW-Server mit selbst signiertem Schlüssel zugreift.
- **Von einer Zertifizierungsstelle (Certification Authority - CA) signiert:** Ein von einer Zertifizierungsstelle wie Thawte, VeriSign oder Commodo gekauftes Zertifikat ist weithin bekannt und der Webbrowser des Benutzers wird es automatisch als vertrauenswürdig einstufen.

Wenn Ihr Server nur von Mitarbeitern verwendet wird, dann ist ein selbst signiertes Zertifikat vielleicht die beste Wahl für Sie. Wenn Sie sicheren Zugriff auf Ihren Webservers vom Internet aus anbieten möchten (z.B. für einen Online-Shop), dann macht es vielleicht Sinn, von einer bekannten Zertifizierungsstelle ein Zertifikat zu kaufen. So können Besucher der Authentizität Ihrer Webseiten vertrauen. In Hinsicht auf die Verschlüsselung sind beide Zertifikate genauso effektiv.

Selbst signiertes Zertifikat erstellen

Um ein selbst signiertes Zertifikat zu erstellen, klicken Sie auf "Selbst signiertes Zertifikat erstellen". Der öffentliche und der private Schlüssel werden in einer gemeinsamen Datei namens "SERVER.PEM" (im Programmverzeichnis von 602LAN SUITE) gespeichert. Ihre SSL-Informationen (Organisationsname, Domänen-Name usw.) werden in der Datei "SSLEAY.CFG" gespeichert. Wenn die Gültigkeitsdauer des Schlüssels abläuft, können Sie jederzeit einen neuen Schlüssel erstellen. Zusätzlich zu den beiden Dateien wird noch die Datei "SERVER.CRT" erstellt, mit der Sie das Zertifikat im Webbrowser (Client) in die Liste der bekannten Zertifikate aufnehmen können.

Certificate Signing Request (CSR) erstellen

Wenn Sie Ihren öffentlichen Schlüssel von einer Zertifizierungsstelle (Certification Authority - CA) zertifizieren lassen möchten, klicken Sie auf "Certificate Signing Request erstellen (CSR)". Wenn das CSR erstellt ist, kopieren Sie es in die Zwischenablage und senden Sie es an Ihre Zertifizierungsstelle, z.B. indem Sie es in das entsprechende Web-Formular oder in eine Mail einfügen. Das Zertifikat, das Sie von der Zertifizierungsstelle erhalten, sollte auf dem 602LAN SUITE-Server gespeichert werden. Klicken Sie dazu auf "Signiertes Zertifikat eingeben", öffnen Sie das empfangene Zertifikat und klicken Sie auf "Zertifikat in 602LAN SUITE speichern".

Erweitert

- **Client-Bestätigung durch Zertifikate** - Aktivieren Sie diese Option, um die Überprüfung des Client-Zertifikates durch die Client-Zertifizierungsstelle einzuschalten. Ansonsten prüft der Client nur das Serverzertifikat. Die folgenden beiden Optionen sind nur anwählbar, wenn diese Option aktiv ist.
- **Zertifikat erforderlich** - Wenn diese Option aktiviert ist, wird für jede weitere Kommunikation die Überprüfung des Client-Zertifikates vorausgesetzt.
- **Nur einmal prüfen** - Ist diese Option aktiviert, akzeptiert der Server nur Zertifikate, die direkt durch die Zertifizierungsstelle (Certificate Authority - CA) bestätigt werden (und nicht durch eine untergeordnete Stelle).
- **Keine Zertifikate verwenden** – Für die Client- oder Server-Authentifikation werden keine Zertifikate verwenden (egal ob selbst oder von einer Zertifizierungsstelle zertifiziert).
- **Server-Zertifizierungsdatei** - Pfad zur Zertifizierungsdatei, die die öffentlichen und privaten Schlüssel enthält.
- **Server-Privatschlüssel** - Wenn die Zertifizierungsdatei den privaten Schlüssel nicht enthält, geben Sie hier den Pfad zu der Datei an, die den privaten Schlüssel enthält.
- **CA-Dateiverzeichnis** - Pfad zum Verzeichnis, das die öffentlichen Schlüssel der Zertifizierungsstellen enthält.
- **CA-Datenbankdatei** - Mehrere öffentliche Schlüssel können auch in einer einzelnen CA-Datenbankdatei zusammengefasst werden. Dies kann geschehen, in dem alle Schlüsseldateien in eine einzelne Datei kopiert werden.
- **Nur SSLv2** – 602LAN SUITE verwendet nur SSLv2.
- **Nur SSLv3** – 602LAN SUITE verwendet nur SSLv3.
- **Keinen temporären RSA-Schlüssel erstellen** – Für die Standard-SSL-Authentifikation wird kein temporärer RSA-Schlüssel erstellt.
- **SSL-Kompatibilität einschalten** – Einige ältere Webbrowser haben einen Fehler in der SSL-Implementierung. Wenn Sie Probleme mit SSL-Verbindungen haben und einen älteren Browser verwenden, versuchen Sie es mit dieser Option.

Sie können verschiedene Verschlüsselungsmethoden (Ciphers) für die Kommunikation zwischen SSL-Server und Clients verwenden. Wählen Sie, welche Methoden der SSL-Server zulassen soll.

Anhang

Befehlssatz Hayes-kompatibler Modems

Nicht alle Modems / Faxmodems unterstützten alle Hayes-kompatiblen Befehle und einige verwenden spezielle Befehle. Diese Information ist für fortgeschrittene Benutzer (für Einwahlverbindungen und Fax-Einstellungen).

Fast alle Befehle beginnen mit den Zeichen "AT" (Achtung - Attention). In einigen Fällen ist Großschreibung erforderlich.

AT Achtung (Attention) – Anfang aller Befehle außer "+ + +", "/A", "A>"
ATA Nimmt die Leitung auf und versucht den eingehenden Anruf zu beantworten.
ATB Wechselt zwischen BELL und CCITT-Standard.
A/ Wiederholt den vorhergehenden Befehl.
A> Wiederholt den vorhergehenden Befehl bis irgendeine Taste gedrückt wird.
ATC Schaltet die Übertragung ein oder aus:
ATC0 Übertragung ausgeschaltet
ATC1 Übertragung eingeschaltet (Standard)

ATD Wählt eine Nummer (Zeichen "," = 2 Sekunden warten). Die folgenden Zeichen können angehängt werden:

- **T** für Tonwahlverfahren
- **P** für Pulswahlverfahren
- **R** Automatisches Antworten (hebt die Leitung direkt nach dem Klingeln ab)
- **W** Auf dem Wählversuch auf den Wählton warten
- **,** Vor nächstem Wählversuch warten (etwas 2 Sekunden – gemäß der Einstellung im S8-Register)
- **@** Verzögerung gemäß Einstellung im S7-Register
- **!** Leitung für 0.5 auflegen und dann weitermachen.
- **;** In den Befehlsmodus schalten (als letztes Zeichen)
- **S** Wählt die im Modem gespeicherte Nummer

ATE Befehlsbestätigung:
ATE0 eingeschaltet – zeige gesendete Zeichen (gedrückte Tasten) an
ATE1 ausgeschaltet
ATF Zwischen Halb-Duplex und Voll-Duplex umschalten:
ATF1 Modem zeigt übertragene Daten an
ATF2 Modem zeigt übertragene Daten nicht an
ATH Auflegen oder Abnehmen:
ATH0 Auflegen
ATH1 Abnehmen
ATI Modem-Informationen zeigen
ATL Setzt die Lautstärke des Lautsprechers:
ATL0 sehr leise
ATL1 leise
ATL2 mittel
ATL3 laut
ATM Lautsprecher an/aus:
ATM0 an
ATM1 an, wenn eine Verbindung aufgebaut wird
ATM2 immer an
ATM3 aus beim Wählen oder beim Empfangen eines Signals
ATO Schaltet in den Datenübertragungsmodus:
ATO0 Schaltet vom Befehlsmodus in den Übertragungsmodus
ATO1 Spezieller geräteabhängiger Befehl
ATQ Antworten auf Befehle zeigen:
ATQ0 eingeschaltet
ATQ1 ausgeschaltet
ATS Modemregister setzen / abfragen:
ATSr=n S-Register "r" auf Wert "n" setzen

ATSr? Liest Wert des S-Registers "r".

ATV Format der Antworten auf Befehle:

ATV0 Numerische Antwort, z.B. 'AT'-(0)

ATV1 alphanumerischer Antwort, z.B. 'AT'-'OK'.

AT>W Modemkonfiguration in internen Speicher speichern

ATX Hayes Smartmodem 300 kompatible Ergebnismeldungen (wie BUSY, CONNECT 9600, usw.)

ATZ Modem zurücksetzen

AT>Z Telefonnummer speichern (wenn möglich). Sie können eine gespeicherte Nummer mit dem ATDS-Befehl wählen.

+ + + Von Übertragungsmodus in den Befehlsmodus wechseln

Beispiel für Mail-Einstellungen

Eine Firma ist mittels Einwähl-Zugang mit dem Internet verbunden. Die Firma hat eine Domäne gekauft, "firma.de", und der Internet-Anbieter hat ein einzelnes POP3-Postfach eingerichtet, das alle Mails an die Domäne enthält. Die Mitarbeiter nutzen MS Outlook Express als Mail-Client.

Lösung: Mails von dem allgemeinen Postfach für die Domäne abrufen

Jeder 602LAN SUITE-Benutzer erhält ein Postfach auf dem 602LAN SUITE-Server. Empfehlenswert ist, Benutzernamen zu wählen, die Teil einer Mail-Adresse sind (z.B. "klaus" für die Mail-Adresse "klaus@firma.de"). Andernfalls ist es erforderlich, den Namen oder die komplette Mail-Adresse als Alias-Adresse des Benutzers einzugeben. Geben Sie im Register "Benutzer" als Standard-Domäne die Domäne der Firma ein. Im Register "POP3" konfigurieren Sie den Abruf des POP3-Postfaches für "firma.de". Wählen Sie "Gemäß der Adresse" für die Option "Empfangene Mails liefern". Outlook Express-Benutzer geben Ihre Mail-Adressen in der Form "name@firma.de" ein. Dies stellt sicher, dass Antworten auf Mails von dem Internet-POP3-Postfach korrekt empfangen werden. Benutzer geben die IP-Adresse des 602LAN SUITE-Servers als POP3- und SMTP-Server an.

Mail-Empfang

Der 602LAN SUITE-Server wird sich ins Internet einwählen und die Mails des Internet-POP3-Postfaches in die internen Benutzer-Postfächer übertragen. Danach kann jeder Benutzer seine Mails vom 602LAN SUITE-Server anfordern.

Mail-Versand

Benutzer erstellen ihre Mails und Outlook Express sendet diese an den 602LAN SUITE-Server. Der Server sammelt diese, wählt sich ins Internet ein und sendet sie ohne Änderung der Absender-Adresse entsprechend der Einstellungen im Register "SMTP".

Problemlösungen

- **Kein SMTP-Relay möglich! (We do not relay)** - Die Mail, die Sie zu senden versuchen stimmt nicht mit Ihren Relay-Einstellungen überein. Die gewöhnlichste Ursache dafür ist, dass die Domäne der Mail-Adresse nicht der Standarddomäne entspricht und auch nicht bei den Benutzer-Aliasen im Register "Benutzer" enthalten ist.
- **DNS: Host nicht gefunden (Host not found)** - Dies tritt auf, wenn Sie eine Mail an eine Domäne senden, die nicht existiert. Prüfen Sie die Mail-Adresse und versuchen Sie es erneut.
- **Kann MX-Einträge für Domäne nicht finden (Unable to locate MX records for domain)** - Sie müssen für Ihre Internet-Verbindung in die Felder "DNS1" und "DNS2" unter "Erweiterte Sendeparameter" im Register "SMTP" bis zu 2 DNS-Server angeben. Wenn Sie die IP-Adressen der DNS-Server nicht wissen, kontaktieren Sie bitte Ihren Internetanbieter.
- **Seit Ihrem letzten Zugriff auf 602LAN SUITE-Webmail hat sich Ihre IP-Adresse geändert. Bitte melden Sie sich erneut an (Your IP address has changed from your last access to the 602LAN SUITE-Webmail. Please login again)** - Dieser Fehler zeigt an, dass die von Ihrem Internetanbieter für Ihre Verbindung zugewiesene IP-Adresse geändert wurde. Dies passiert typischer bei großen Internetanbietern wie AOL, die anstatt direkten Verbindungen Proxyserver verwenden, um Webseiten zu holen. Sie müssen einen anderen Internetanbieter verwenden, um auf den Webmail-Dienst zuzugreifen.
- **Server-Zertifizierungsdatei nicht definiert (Server Certificate File is not defined)** - Dies geschieht, wenn Sie SSL-Dienste aktiviert haben, aber auf dem Server kein SSL-Zertifikat erstellt haben. Erstellen Sie ein SSL-Zertifikat, um das Problem zu beheben (Register "SSL").
- **Kann AVG Anti-Virus nicht initialisieren (Error: Cannot initialize AVG kernel)** – Das bedeutet, dass das Programm AVG Anti-Virus nicht auf dem Server installiert wurde oder die Installation defekt ist. Das Problem lässt sich in der Regel durch eine Neu-Installation lösen.
- **"Übertragung unterbrochen" beim Versuch ein Fax zu senden ("Transmission Interrupted" error message when sending a fax)** - Dieser Fehler kann durch drei Faktoren ausgelöst werden: Rauschen auf der Leitung, ein inkorrektes Windows-Modem-Profil oder ein ungeeigneter Modem-Initialisierungs-String. Ihre Telekommunikationsfirma kann helfen, das Rauschen auf der Leitung zu minimieren und Ihr Modem-Hersteller sollte Ihnen ein passendes Modem-Profil und einen optimierten Initialisierungs-String anbieten können. 602LAN SUITE unterstützt keine CAPI-Modems und keine virtuellen TAPI-Modems, wie Sie oft von ISDN- oder CAPI-Modems erstellt werden.
- **SendFax-Client: Kann Programm zum Faxversenden nicht starten (Unable to run program for sending fax)** - Dies tritt auf, wenn der SendFax-Client nicht mit dem 602LAN SUITE-Server kommunizieren kann. Dies passiert gewöhnlich, wenn der SMTP-Server ausgeschaltet ist, ein anderer SMTP-Server bereits den SMTP-Port 25 belegt oder die IP-Adresse des 602LAN SUITE-Servers geändert wurde. Der SMTP-Server kann im Register "SMTP" eingeschaltet werden. Versuchen Sie den Server von einem anderen Computer aus anzupingen. Lesen Sie "Kann SMTP-Server nicht initialisieren" für Informationen, wie Sie einen Port-Konflikt lösen können.
- **Kann SMTP-Server nicht initialisieren (Port bereits belegt?)** – 602LAN SUITE kann den SMTP-Port (Port 25) nicht öffnen. Dies kann durch ein anderes Programm verursacht werden, das den SMTP-Port verwendet, wie z.B.: Der SMTP-Dienst von Internet Information Services (IIS) oder Norton Anti-Virus sowie verschiedene Viren oder trojanischen Pferden mit eingebautem SMTP-Server (Sircam, Iloveyou, usw.).

Exklusiv-Vertrieb für Deutschland, Österreich & Schweiz:

HAAGE & PARTNER Computer GmbH
Schlossborner Weg 7
61479 Glashütten
Deutschland

Telefon: (06174) 966 100
Telefax: (06174) 966 101

Internet: www.haage-partner.de oder www.software602.de

Händleranfragen: dealers@haage-partner.de